

AirDefense Personal 3.4

Manager User Guide



AirDefense Personal 3.4 Manager User Guide

This document is to be used exclusively by AirDefense employees, authorized dealers, customers and distributors of AirDefense products.

The information in this manual is subject to change without notice and should not be construed as a commitment by AirDefense. AirDefense shall in no event be liable for any loss of business, loss of use or data, interruptions in business or for damage of any kind arising from any defect or errors in this publication or in the AirDefense hardware or software.

This material may not be reproduced in whole or in part by any means without permission from AirDefense.

All other trade names not listed above and referenced in this document are the service marks, trademarks, or registered trademarks of their respective manufacturer(s) and belong to their respective owner(s).

Copyright © 2007 AirDefense. All rights reserved.

AirDefense, Inc.
4800 Northpoint Parkway, Suite 100
Alpharetta, GA 30022

Online Support

The AirDefense GUI provides a link that enables you to access the Support Center; to Open New Cases; to View Cases; and to access the self support site to search for solutions.

Click on the help icon and pull down the help menu. Choose **Support**. Click on **Open** or **View Cases**. Or you can access online support at <http://support.airdefense.net>.

Call Center Support

AirDefense is available to you 24x7 via our Online Customer Care Tracking System, AirDefense's Support Desk, or Email. Hours of service and response times are subject to customer care contract terms.

- Call Center Support 800.913.1257
- International callers: +1 306.791.5673
- Online Customer Care Tracking: <http://support.airdefense.net>

Email

Technical Support may be reached by email, at Support@AirDefense.net.

Table of Contents

Chapter 1. Before You Begin.....	1-1
About this Manual	1-1
Additional Resources	1-1
Chapter 2. Getting Started.....	2-1
About the AirDefense Personal Manager	2-1
About the AirDefense Personal System	2-1
Integration with AirDefense Enterprise	2-1
Using the Menu	2-1
Summary of Menu Bar Options	2-2
File	2-2
Tools	2-2
Print Charts	2-2
Help	2-2
Using the File Option.....	2-2
Using the Tools Option.....	2-3
Using Wizards	2-3
Using Upgrade License	2-3
Using Set Refresh Time Interval.....	2-3
Using Refresh.....	2-3
Using the Print Screens Option	2-3
Print Preview - Graph:	2-4
To set up the printing of a graph:	2-5
Using the Help Option	2-6
Chapter 3. Agent List.....	3-1
Agent Filter	3-1
Color Coding	3-2
Group Operations.....	3-2
Data Search	3-2
Data Export	3-4
Agent Details	3-4
Threat Status Details	3-6
To Access Threat Status:	3-6
Alert History Details	3-7
To Access Alert History	3-7
Last Scan and Scan Frequency	3-7
To Display Alarms by Specific Day.....	3-8
To Display Specific Severity Levels of Alarms	3-8
Alert Counts.....	3-8
Export Alert History.....	3-8
Threat Level History Details	3-9
To Access Alert History	3-9
Alarm History Details	3-10
To Access Alarm History	3-10
Wireless Status Details	3-11

To Access Wireless Status	3-11
Current Wireless Status.....	3-11
Wireless LAN Status.....	3-11
Wireless Status History Details	3-12
To Access Wireless Status History.....	3-12
Chapter 4. Using the Manager Graph Tabs	4-1
Using the Threat Level Tab	4-1
To Access the Threat Level Table.....	4-3
Using the Device Usage Tab	4-3
To Access the Device Usage Table	4-5
Using the Policy Violation Tab	4-5
To Access the Policy Violation Table	4-7
Using the Alarms Tab.....	4-8
To Access the Alarms Table	4-9
Chapter 5. Wizards	5-1
Using the Rule Wizard	5-1
New Rule or Edit Rule	5-2
Hotfix Rule.....	5-4
Process Rule	5-6
Registry Rule.....	5-8
Device Rule	5-11
Network Rule.....	5-13
Delete Rule.....	5-14
Response Wizard	5-16
New Response or Edit Response	5-17
Delete Response.....	5-18
Policy Wizard	5-19
New Policy or Edit Custom Policy	5-20
Delete Policy	5-23
Profile Wizard	5-24
Create New Profile or Edit Profile.....	5-25
Delete Profile	5-31
Group Wizard	5-32
Groups Wizard	5-32
New Group	5-33

Chapter 1. Before You Begin

About this Manual

This guide describes the information needed to successfully operate AirDefense Personal Manager.

Additional Resources

- Registered users can logon to <http://support.airdefense.net/> and view technical documentation
- User Guides
- Install Guides
- Quick Install Guides
- Policy Guides

Chapter 2. Getting Started

Welcome to the AirDefense™ Personal Manager™, the key to effectively administering and monitoring activities for all AirDefense Personal Agents.

About the AirDefense Personal Manager

Using the Personal Manager, you can:

- Centrally define and update policy
- Automatically enforce wireless laptop security policy
- Dashboard view of alarms, threat level, policy violations, and devices
- Usage summary
- Set up profiles
- View Personal Agents
- View various operating parameters for Agents
- Monitor performance and system health statistics in your wireless network
- Serves as the interface to the AirDefense Personal Server

About the AirDefense Personal System

Profiles that are defined in AirDefense Personal Manager are automatically transmitted to each AirDefense Personal Agent. If threats are discovered, the AirDefense Personal system can be configured to notify the user and send logs to the Personal Manager for central reporting and notification.

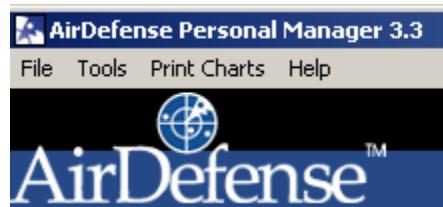
Integration with AirDefense Enterprise

The database component of AirDefense Personal can also simultaneously run on an existing AirDefense Enterprise Server.

Once integrated, the Enterprise Graphical User Interface (GUI) can display all AirDefense Personal alarms. Alarms normally seen on the AirDefense Personal Agent and Manager can be viewed in the Enterprise GUI.

Using the Menu

The **Menu Bar** occupies the left-hand side of the AirDefense Personal Manager Graphical User Interface main screen. The Menu Bar contains drop-down menus that provide options and functionality for the program.



Summary of Menu Bar Options

File

File allows you to exit out of the system by clicking on **Exit**.

Tools

Tools allow you to do the following:

- Use the Rule Wizard
- Use the Response Wizard
- Use the Policy Wizard
- Use the Profile Wizard
- Use the Groups Wizard
- Upgrade Licenses
- Set a Refresh Time Interval
- Refresh the system

Print Charts

Print Charts allows you to print each tabbed graph (or chart) displayed on the main window--Device Usage, Threat Level, Policy Violation, and Alarms. The following tasks from this menu option are available:

Print Preview – Preview a print job before sending it to the printer

Page Setup - Configure print jobs

Print – Print selected charts

Help

Displays the help system and its contents.

Using the File Option

1. Use **File>Exit** to exit from the system.



2. Go to **File** and click on **Exit**.

AirDefense Personal Manager ends the monitoring session and saves all current settings. Although you will not be able to see AirDefense Personal Manager the AirDefense Personal Server will continue to operate.

Using the Tools Option

The selections available in the Tools Menu enable Administrators to perform most of the key features in the AirDefense Personal Manager.



Using Wizards

To launch one of the wizards, simply select it from the tools menu. Wizard functionality is covered in more detail in Chapter 5.

Using Upgrade License

To Upgrade the AirDefense Personal Manager License, Go to **Tools > Upgrade License**. The AirDefense Personal License dialog displays with a field to enter a new license key. Enter the key and click **<OK>**.

Using Set Refresh Time Interval

Go to **Tools > Set Refresh Time Interval**. A Refresh screen appears that enables you to set an automatic refresh time in minutes. Enter a time in minutes from the selector and click **<Apply>**.

Using Refresh

Go to Tools and click on **<Refresh>**. All data displayed will be refreshed Tools > Refresh pulls the latest data into AirDefense Personal Manager from the server.

Using the Print Screens Option

Go to **Print Charts** and select the type of chart (Device Usage, Threat Level, Policy Violation, or Alarms) and the print option. You can select Print Preview, Page Setup, and Print.

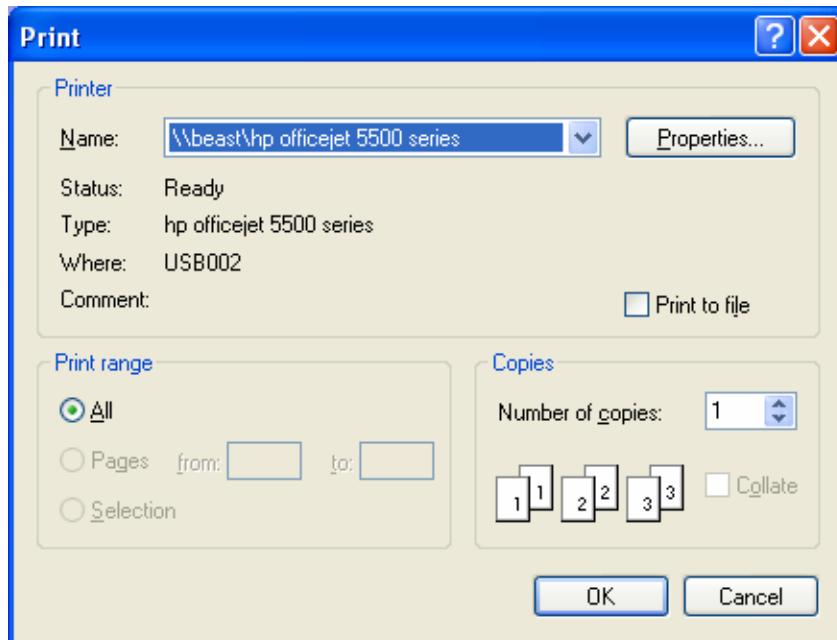
- If Select **Print Preview**, to preview a graph.
- Select **Page Setup**, to access a Page dialog that allows setting page dimensions and orientation a print job.
- Select **Print**, to display a Print dialog which allows you to start a print job.

Use the steps below to complete each task.

To print a graph:

1. Click on the **Print Chart** menu option, select one of the four available graphs, and use the right-arrow to select **Print**.

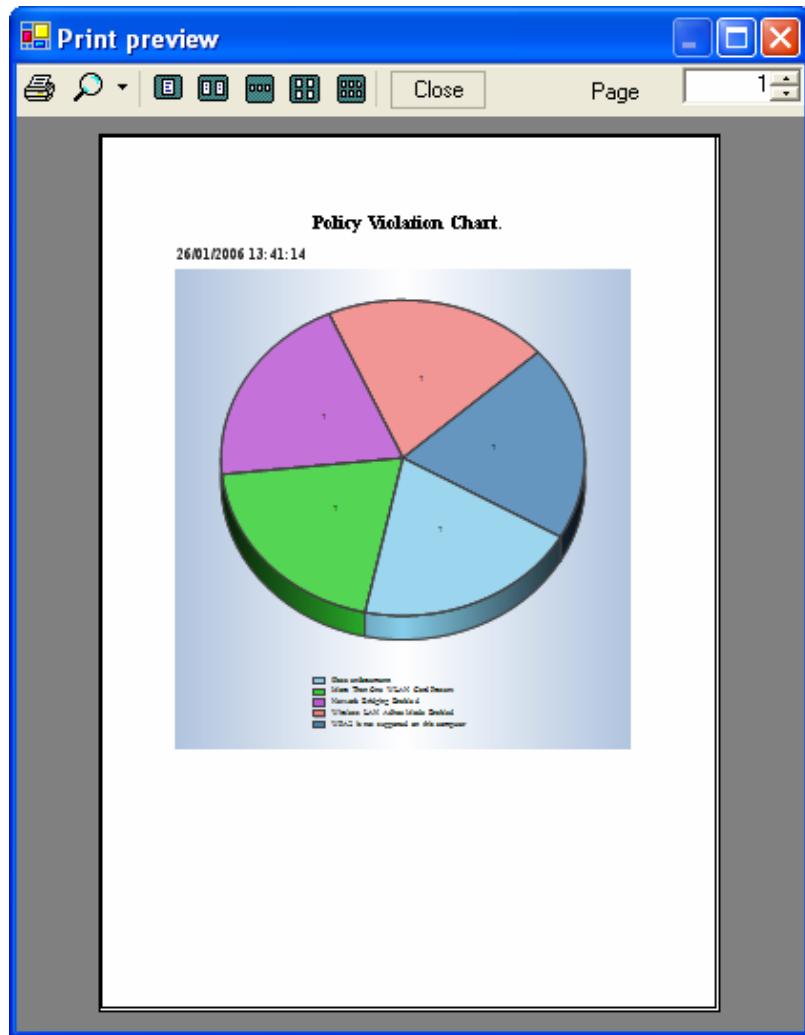
The **Print** dialog displays.



2. Select the desired print options such as Printer, Print Range, and number of copies.
3. Click on **OK** to start the print job.

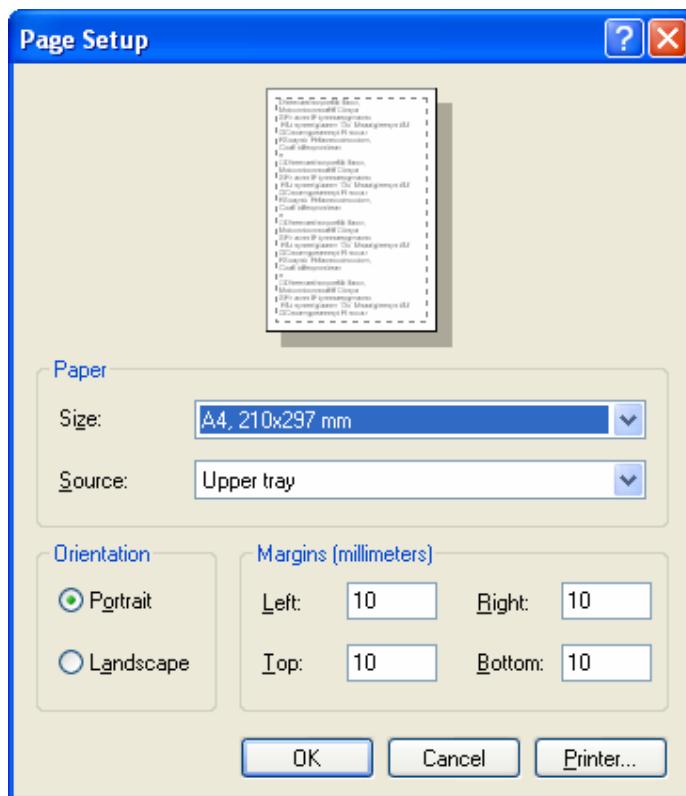
Print Preview - Graph:

1. Click on the **Print Chart** menu option; select one of the four available graphs to print, and use the right-arrow to select **Print Preview**.
2. The **Print Preview** dialog displays the selected.



To set up the printing of a graph:

1. Click on the **Print Chart** menu option; select one of the four available graphs to print, and use the right-arrow to select **Print Preview**.
2. The **Print Preview** dialog displays with the selected graph in the preview section of the dialog.
3. The **Page Setup** dialog displays.

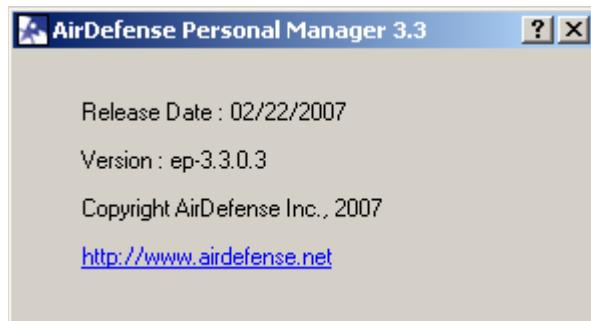


4. Select the desired page setup options such as Paper, Orientation, and Margins.
5. Click on **OK** to save settings.
6. Click on **Printer** to start printing process.

Using the Help Option

Go to **Help** and click on the AirDefense Personal Manager Help option to access the Help system.

Click on the **About** option to display a dialog detailing brief specifics about your version of the AirDefense Personal Manager application.

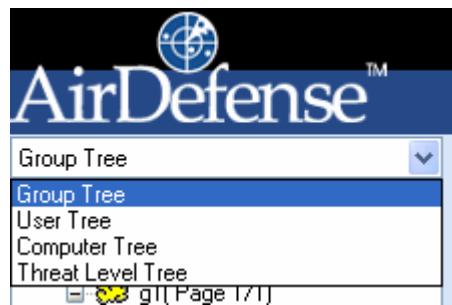


Chapter 3. Agent List

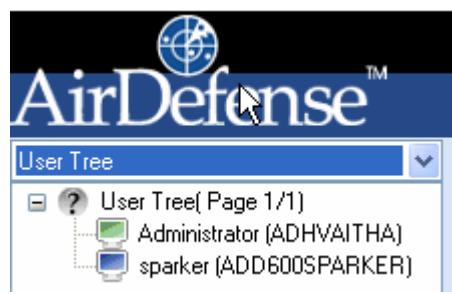
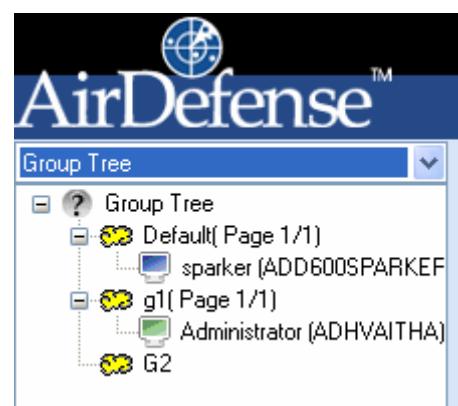
The Agent List is a list of Agents in your system. Through the Agent List, you can display an Agent Detail dialog for each Agent in your AirDefense Personal system.

Agent Filter

Using the filter selection at the top of the tree, you can display the contents of the Agent List by Threat Level, by User Name, by Computer Name, or by Group Name.



The illustrations below show examples of these views.



Color Coding

Each Agent is represented by a color-coded icon. Each color represents a Threat Level:

- Severe = Red
- High = Orange
- Elevated = Yellow
- Guarded = Blue
- Low = Green

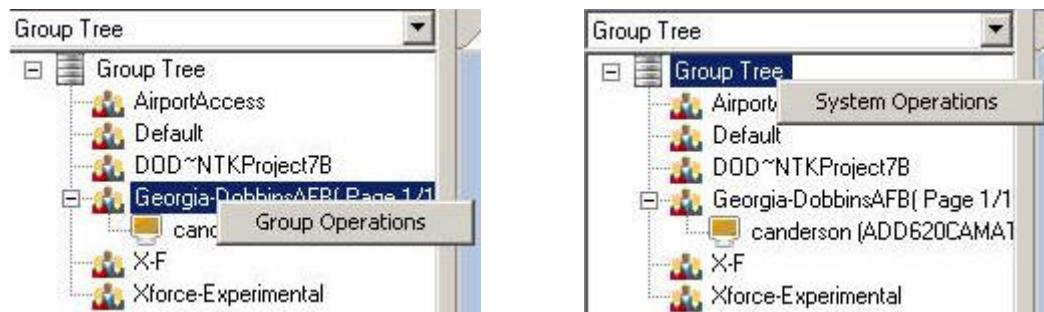


Group Operations

Data Search

The ability to search for data is included in Group Operations and System Operations. Group Operations can be used to search the highlighted group. System Operations will search the entire system. To initiate a search, right-click on a group and select **Group Operations**, or highlight at the system level and select **System Operations**.

Note: Starting with a higher level group expands your search.



The System Data window is displayed. This is where you define your search. The following search fields are available:

Field	Description
Search Based On	Searches are based on the column headings. They are: <ul style="list-style-type: none"> • User Name • Computer Name • Agent ID • Last Seen Time • Group Name • Profile Name • Critical Alarm • Major Alarm • Minor Alarm • Ignore Alarm
Sort Order	You may select ascending or descending search.
Sort Results Based On	You can sort the results based on the column headings list above.
Show	The total amount of records to be displayed as a group. You may select: <ul style="list-style-type: none"> • 10 • 100 • 200 • 500 • 1000
Search String	A specific string to search for. If this field is blank, search for all is assumed.

After specifying all your search criteria, click the <**Search**> button to display the search data. Once the data is displayed, you can view more specific details by double-clicking on one of the agents. You can also right-click on the agent to display more details. These options are discussed in detail under [Agent Details](#).

You can select (highlight) two or more agents by sweeping them. Left-click in the white space next to (left) the first agent while continuing to hold the mouse button, move the cursor to the last agent that you want to select and then release the mouse button. Once you have made your selection, you can delete or move the agents by right-clicking in the highlighted area.

Data Export

Group Operations also includes a data export feature. This feature allows you to save all data from your search to a CSV file. Just click the <Export> button and follow the prompts.

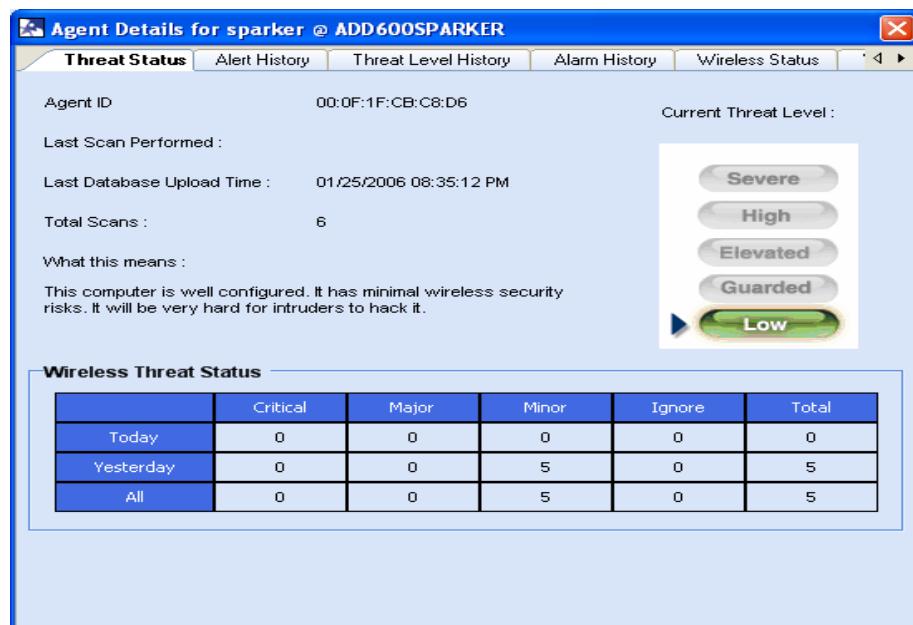
Another way to export data is to click on any graph in the dashboard view to display a table view of the graph. While in table view, you can export data all the data for the agents listed with the <Export> button located at the bottom of the table.

Once you save the file, you can open it in Excel or any other program that will read and format a CSV file.

Agent Details

You should select the ordering desired by Group, User, Threat Level or User. To see agent details double-click on an Agent in the Agent List. The Agent Detail dialog displays six tabs that contain detailed information about the Agent. The tabs are:

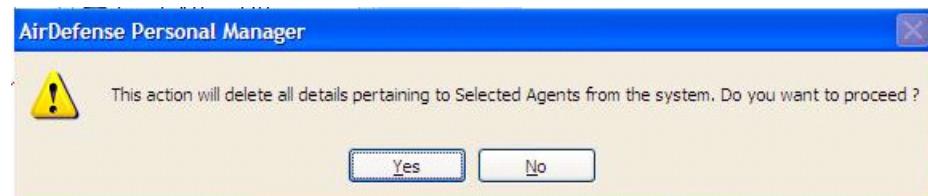
- **Threat Status** displays the scan and threat status.
- **Alert History** displays the Alert information such as counts.
- **Threat Level History** displays the alarm count and threat level information.
- **Alarm History** displays the Alarm information such as counts and severity.
- **Wireless Status** displays the current wireless and wireless LAN status.
- **Wireless Status History** displays past wireless and wireless LAN status.



You can also access the Agent Details screen by right-clicking on the Agent in the List view and selecting Agent Details.



From this menu you can also delete all of the Agent information from the Database. You will be asked if you want to delete all of the details pertaining to this agent in the database. Select the **Delete** button to confirm this action.



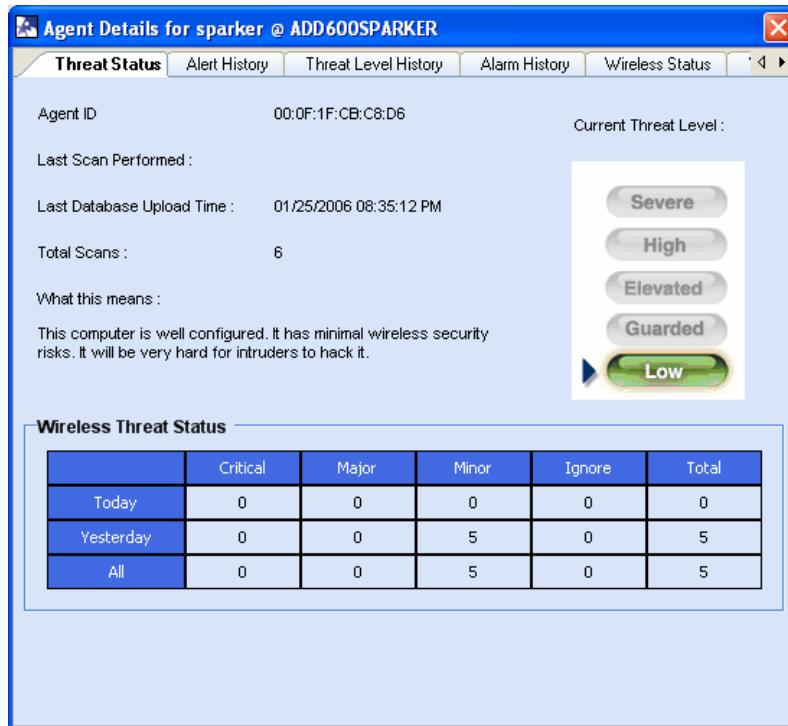
If the Agent is still active then the next time the agent uploads information it will reappear in the Default group and it will download the profile for the Default group and run that until it is moved into a different group.

Threat Status Details

Use the **Threat Status** tab to view current threat detail information for the selected agent.

To Access Threat Status:

1. Either double click on an agent in the Agent list or click on one of the graphs and then double click on one of the data rows to see the Agent Details.
2. Click on the **Threat Status** tab.



The **Threat Status** tab displays:

- The Agent ID
- The date and time the last scan was performed on the Agent
- The Current Threat Level
- The Total Scans performed
- An explanation of the Current Threat Level
- A Wireless Threat Status table that displays all alarms received today and yesterday.

Alert History Details

Use the **Alert History** tab to view the Alerts generated by the selected Agent. The **Alert History** tab displays Alerts, Alert Counts, and Severity Levels.

To Access Alert History

1. Either double click on an agent in the Agent list or click on one of the graphs and then double click on one of the data rows to see the Agent Details.
2. Click on the **Alert History** tab.

Alarm Raised Time	Database Upload Time	TimeZone	Severity	Name	Cab
01/25/2006 08:30:08 PM	25/01/2006 20:32:16	GMT 00: 00	Minor	Wireless Conn...	Risk
01/25/2006 08:30:08 PM	25/01/2006 20:32:16	GMT 00: 00	Minor	Wireless LAN ...	Risk
01/25/2006 08:30:08 PM	25/01/2006 20:32:16	GMT 00: 00	Minor	Connected to ...	Risk
01/25/2006 08:30:08 PM	25/01/2006 20:32:16	GMT 00: 00	Minor	Connected to ...	Risk
01/25/2006 08:30:08 PM	25/01/2006 20:32:16	GMT 00: 00	Minor	No Encryption...	Inse

Last Scan and Scan Frequency

The Agent's Alert History displays the Last Scan date and time, and the Scan Frequency (time between scans).

To Display Alarms by Specific Day

Click on the drop-down arrow in the **Show** field and select either:

- Most Current Alarms
- Today's Alarms
- Yesterday's Alarms
- All Alarms

The alarms will display in the table at the bottom of the **Alert History** dialog. The Alarms are displayed by Alarm Raised date and time, Database Upload date and time, Time Zone, Severity, Name and Category.

To Display Specific Severity Levels of Alarms

Click on the drop-down arrow in the **Severity** field, and select either:

- Ignore
- Minor
- Major
- Critical
- All

Depending on the Severity Level selected, the appropriate Alerts Severity Levels will be displayed.

Alert Counts

The **Alert Counts** section of this dialog displays the number of Alarms for each Severity Level.

Export Alert History

You can export all of the Alert History by clicking the <**Export**> button at the bottom of the **Alert History** tab and following the prompts. The data is exported as a CSV file.

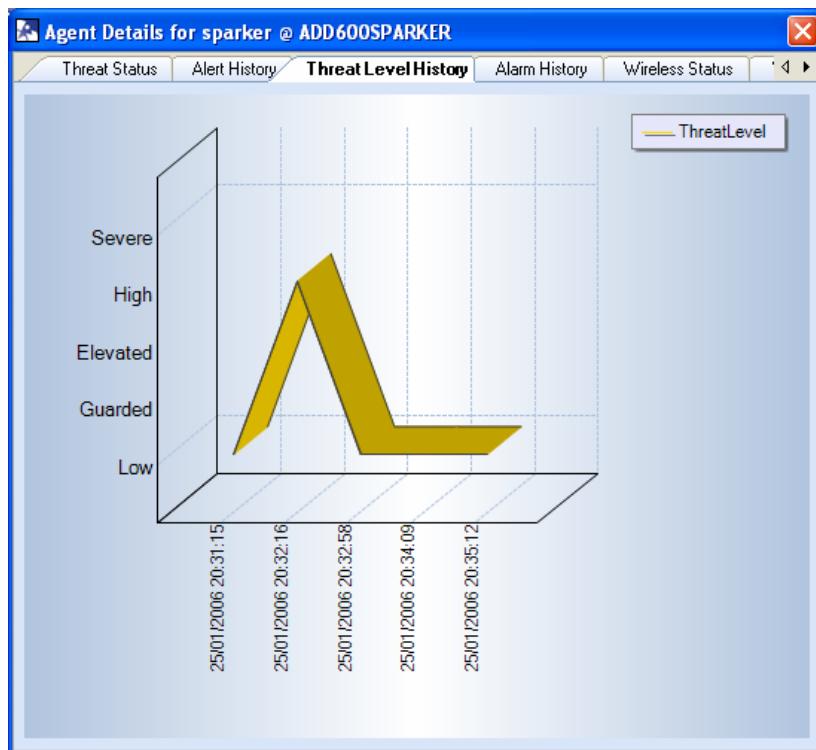
Once you save the file, you can open it in Excel or any other program that will read and format a CSV file.

Threat Level History Details

Use the **Threat Level History** tab to view Threat Levels for a selected Agent across a historical time line.

To Access Alert History

1. Either double click on an agent in the Agent list or click on one of the graphs and then double click on one of the data rows to see the Agent Details.
2. Click on the **Threat Level History** tab



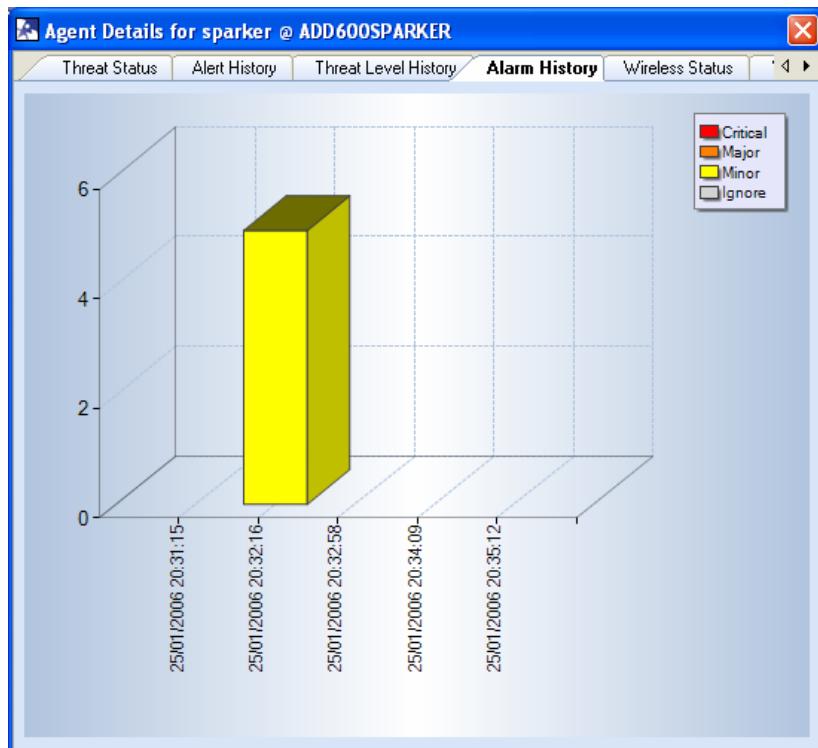
The graph displays the cumulative Threat Levels generated by the selected Agent by date and time.

Alarm History Details

Use the **Alarm History** tab to view the Alarms generated on a selected Agent. The **Alarm History** tab displays color bars that indicate the number and severity of alarms for the dates and times indicated.

To Access Alarm History

1. Either double click on an agent in the Agent list or click on one of the graphs and then double click on one of the data rows to see the Agent Details.
2. Click on the **Alarm History** tab.

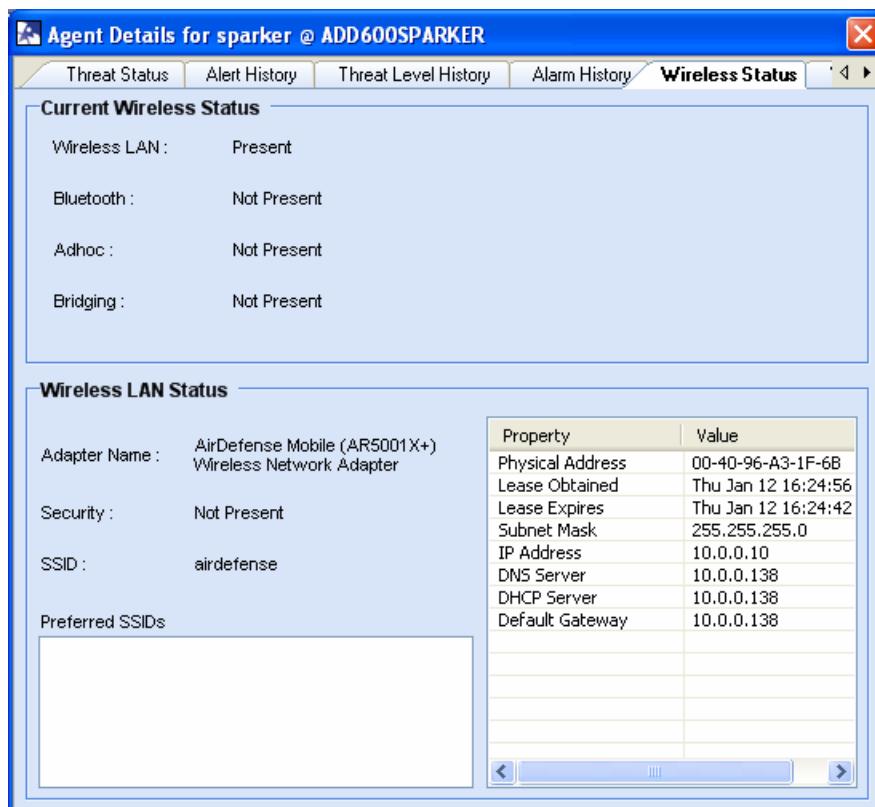


Wireless Status Details

The **Wireless Status** tab displays the status of your wireless devices and your wireless local area network.

To Access Wireless Status

1. Either double click on an agent in the Agent list or click on one of the graphs and then double click on one of the data rows to see the Agent Details.
2. Click on the **Wireless Status** tab to access the Agent's wireless status.



Current Wireless Status

The **Current Wireless Status** section displays each type of wireless device. It illustrates if a device is present or not in your system, and if it is currently enabled or disabled.

Wireless LAN Status

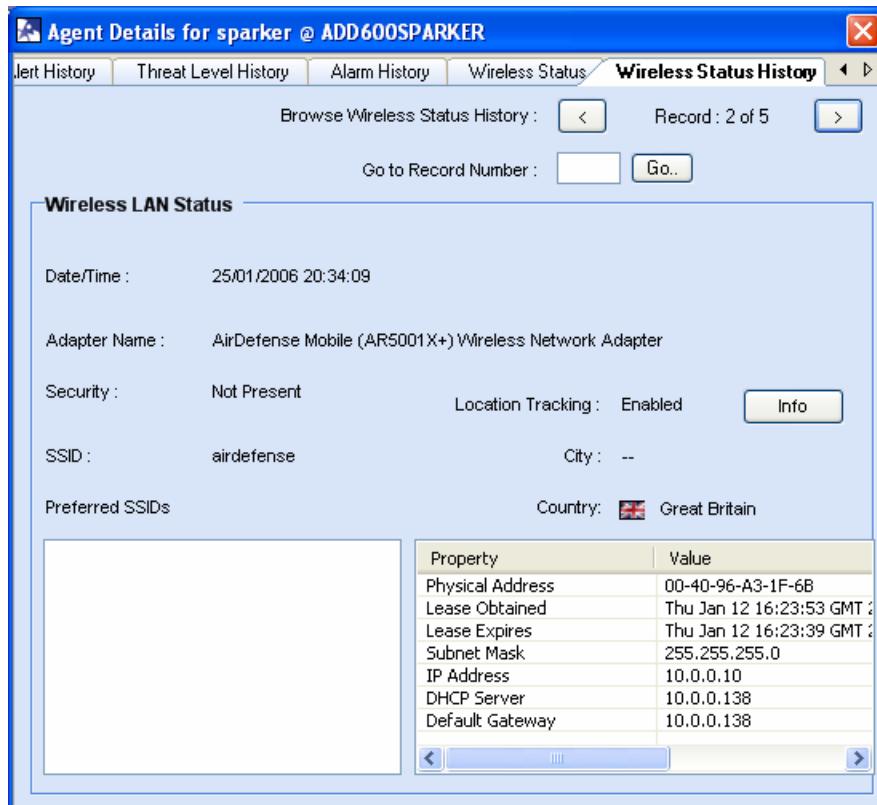
The **Wireless LAN Status** section displays information about your wireless local area network such as Adapter Name, Security, and SSID. Additionally, Preferred SSIDs and Lease history displays in two viewing windows.

Wireless Status History Details

Use the **Wireless Status History** tab to display the historical status of your wireless devices and your wireless local area network.

To Access Wireless Status History

1. Either double click on an agent in the Agent list or click on one of the graphs and then double click on one of the data rows to see the Agent Details.
2. Click the **Wireless Status History** tab to access the Agent's wireless status history.



To advance to the next record, click on the right arrow at the top of the window. To go back, click on the left arrow.



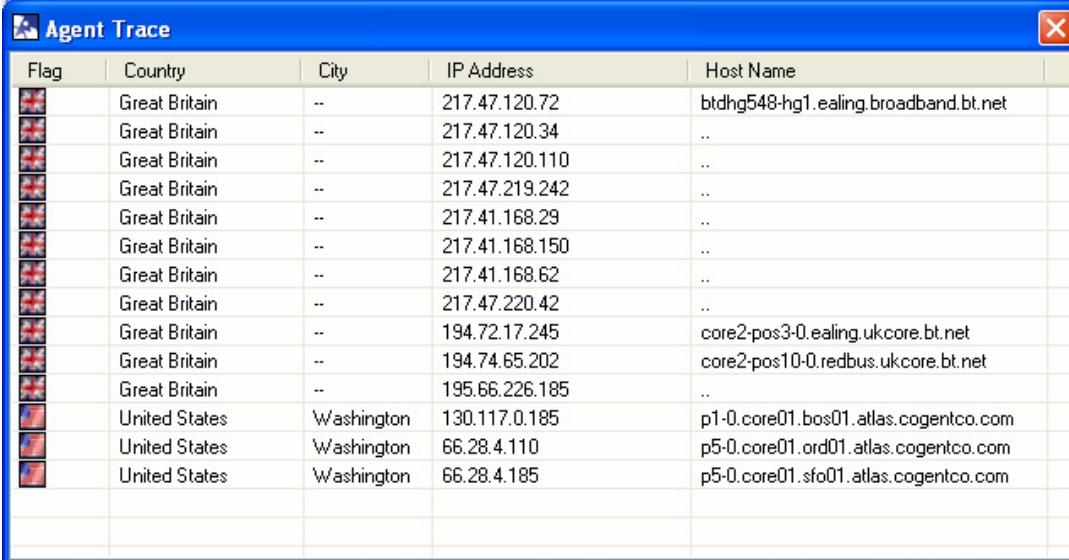
You have the option of going directly to a particular record if you know the record number by entering the number in the entry box.

The Wireless LAN Status section displays the following information: on the

- **Date/Time:** Current date and time, based on the AirDefense Personal Manager computer setting.
- **Adapter Name:** The type of adapter.
- **Security:** Wireless security settings for the Personal Manager, for example, WEP.

- **Preferred SSIDs:** List of the AirDefense Personal Manager computer's SSID preferences.
- **Lease Information:** This table displays the historical lease information for this AirDefense Personal Manager computer.
- **Location Tracking:** If agent tracing is enabled in the profile, you can access the trace route information by clicking the **Info** button. If a city or country is available for the IP address you will see this displayed here.

The **Location Tracking Info** button will display a record of the trace route from the agent to the given IP address or URL.



The screenshot shows a Windows-style dialog box titled "Agent Trace". It contains a table with five columns: Flag, Country, City, IP Address, and Host Name. The table lists 15 rows of data, mostly from Great Britain, with one row from the United States. The "Flag" column shows small icons representing the countries. The "Country" column lists "Great Britain" 14 times and "United States" once. The "City" column shows either "--" or the city name. The "IP Address" column lists various IP addresses. The "Host Name" column lists domain names like "btihg548-hg1.ealing.broadband.bt.net" and "core2-pos3-0.ealing.ukcore.bt.net".

Flag	Country	City	IP Address	Host Name
GB	Great Britain	--	217.47.120.72	btdhg548-hg1.ealing.broadband.bt.net
GB	Great Britain	--	217.47.120.34	..
GB	Great Britain	--	217.47.120.110	..
GB	Great Britain	--	217.47.219.242	..
GB	Great Britain	--	217.41.168.29	..
GB	Great Britain	--	217.41.168.150	..
GB	Great Britain	--	217.41.168.62	..
GB	Great Britain	--	217.47.220.42	..
GB	Great Britain	--	194.72.17.245	core2-pos3-0.ealing.ukcore.bt.net
GB	Great Britain	--	194.74.65.202	core2-pos10-0.redbus.ukcore.bt.net
GB	Great Britain	--	195.66.226.185	..
US	United States	Washington	130.117.0.185	p1-0.core01.bos01.atlas.cogentco.com
US	United States	Washington	66.28.4.110	p5-0.core01.ord01.atlas.cogentco.com
US	United States	Washington	66.28.4.185	p5-0.core01.sfo01.atlas.cogentco.com

Chapter 4. Using the Manager Graph Tabs

The four tabs that display on the AirDefense Personal Manager main menu enable you to monitor various performance and system health statistics of your wireless network.

- **Threat Level Graph** – Displays the threat levels and number of threats received against Agents in your system.
- **Device Usage Graph** – Displays all the devices being used by Agents in your system.
- **Policy Violation Graph** – Displays all the policies being violated by all the Agents in your system.
- **Alarms Graph** – Displays the number and types of alarms that Agents on your system are generating.



Right-Click Option

Right clicking on a chart gives you a table that lists statistics for that tab.



Double-Left-Click Option

If you double-left-click on a particular row on the table (each row pertains to a specific Agent) the **Agent Details** screen is displayed.

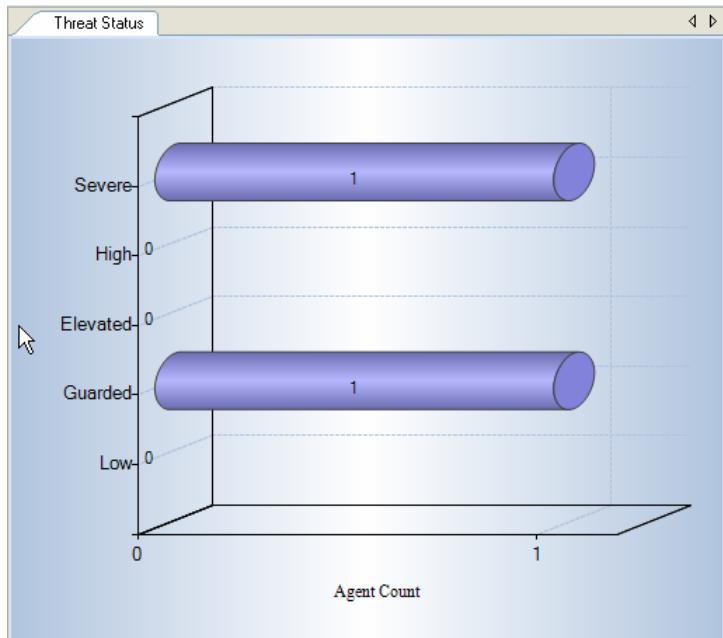
Using the Threat Level Tab

The **Threat Level** tab displays the threat levels and number of threats received against Agents in your AirDefense Personal system. You can view a graph that summarizes the information or a more detailed table.

The graph shows:

- The number of threats.
- The color-coded threat level of the threats received.
- The number of Agents polled.

Example: The graph below shows that there are currently one elevated, one Guarded, and one Low threat against two Agents in the system.



Right-click on one of the bars in the graph to view this information as a table:



Double-left-click on a row to view the **Agent Detail** screen an Agent.

The **Previous** and **Next** buttons page allow you to see more devices in this view. You can choose the number of device per page by selecting this from the drop-down box.

Right-click on the table brings you back to the display to the graph view.



To Access the Threat Level Table

To access the table, place your mouse on any bar in the graph and right-click. The table displays the following information.

Entries in the table are color-coded according to their severity level (Severe, High, Elevated, Guarded, Low).

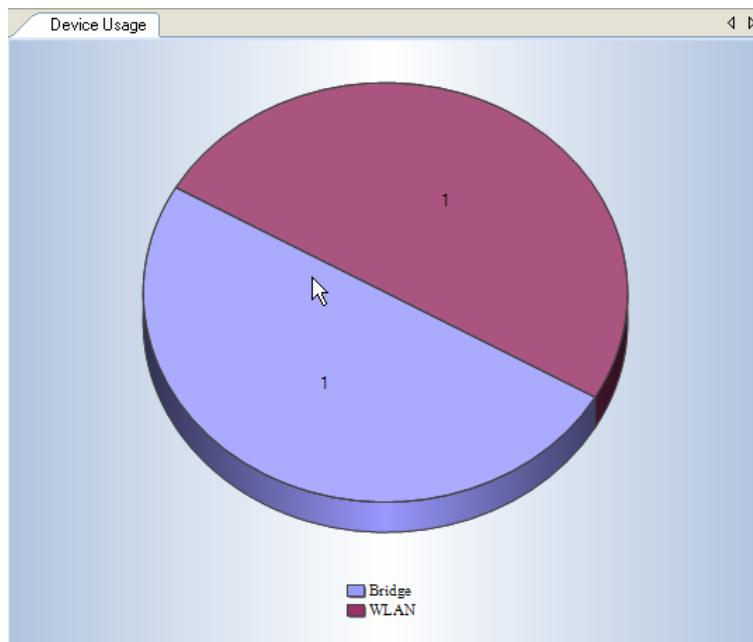
Column	Meaning
User Name	The user name assigned to this Agent.
Computer Name	The alpha or numeric computer name of this Agent.
Threat Level	The threat level for this Agent. (Severe, High, Elevated, Guarded, or Low)
Agent ID	The MAC address of this Agent.
Last Seen	The last date and time this alarm was generated for this Agent, in the format: mm/dd/yyyy hh:mm:ss am/pm .
Critical	The number of Critical alarms generated for this Agent.
Major	The number of Major alarms generated for this Agent.
Minor	The number of Minor alarms generated for this Agent.
Ignore	The number of Ignored alarms generated for this Agent.

Using the Device Usage Tab

The Device Usage tab displays an overview of all the different types of devices that are being used by all of the Agents in your AirDefense Personal system. You can view a graph that summarizes the information or a more detailed table.

The graph shows:

- The number of each type of device in use.
- The type of device by color code.



Right-click on one of the segments in the graph to view chart information as table.

A table titled "Device Usage" showing detailed information for a single device. The table has columns for User Name, Computer Name, Threat Level, Agent ID, Last Seen, and Critical Alarms. The first row shows the data for a device named "sparker". At the bottom of the table are navigation buttons for "Prev", "100", a dropdown menu, and "Next".

User Name	Computer Name	Threat Level	Agent ID	Last Seen	Critical Alarms
sparker	ADD600SPARKER	Guarded	00:0F:1...	11/07/20...	0



Double-left-click a row to display for the detailed information.

The **Previous** and **Next** buttons page allow you to see more devices in this view. You can choose the number of device per page by selecting this from the drop-down box.



Right-click on the table to return to the graph view.

To Access the Device Usage Table

To access the table, place your mouse on any segment in the chart and right-click. The table displays the following information.

Entries in the table are color-coded according to their severity level (Severe, High, Elevated, Guarded, Low).

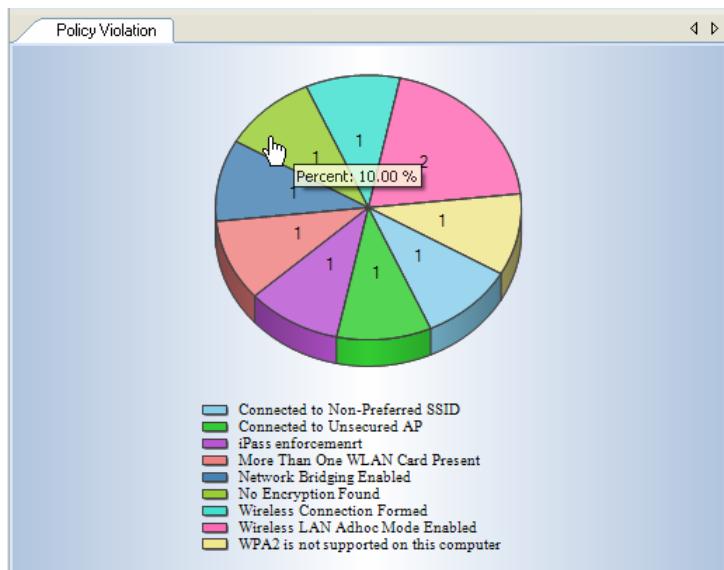
Column	Meaning
User Name	The user name assigned to this Agent.
Computer Name	The alpha or numeric computer name of this Agent.
Threat Level	The threat level for this Agent. (Severe, High, Elevated, Guarded, or Low)
Agent ID	The MAC address of this Agent.
Last Seen	The last date and time this alarm was generated for this Agent, in the format: mm/dd/yyyy hh:mm:ss am/pm .
Critical	The number of Critical alarms generated for this Agent.
Major	The number of Major alarms generated for this Agent.
Minor	The number of Minor alarms generated for this Agent.
Ignore	The number of Ignored alarms generated for this Agent.

Using the Policy Violation Tab

The **Policy Violation** tab displays all of the policies that are being violated by all of the Agents in your AirDefense Personal system. You can view a graph that summarizes the information or a more detailed table. Policies are color-coded according to the color key on the chart.

The graph shows:

- The policy violations being generated
- The number of Agents generating the policy violations
- A color-coded policy key



Right-click on one of the segments in the graph to view this information as a table.



Double-left-click on a row to view the **Agent Details** screen for that Agent.

The **Previous** and **Next** buttons page allow you to see more devices in this view. You can choose the number of device per page by selecting this from the drop-down box.

Right-click on the table to return to the graph view.



To Access the Policy Violation Table

To access the table, place your mouse on part of the colored pie chart and right-click. The table displays the following information.

Entries in the table are color-coded according to their severity level (Severe, High, Elevated, Guarded, Low).

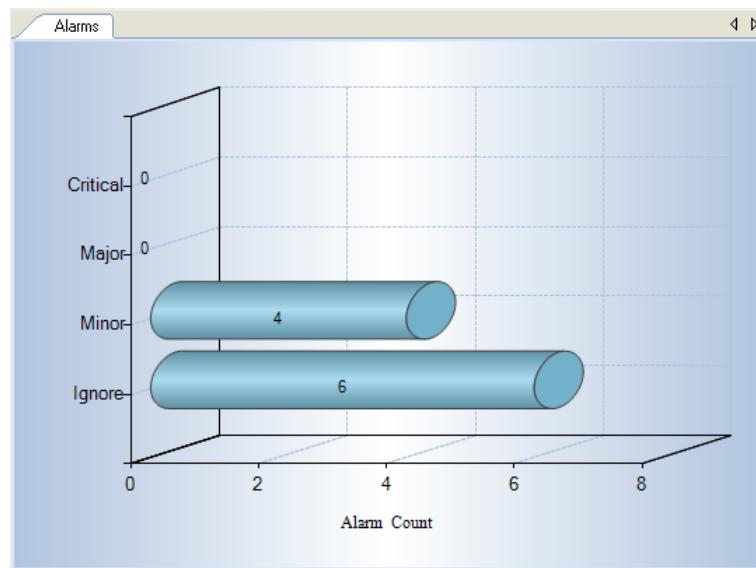
Column	Meaning
User Name	The user name assigned to this Agent.
Computer Name	The alpha or numeric computer name of this Agent.
Threat Level	The threat level for this Agent. (Severe, High, Elevated, Guarded, or Low)
Agent ID	The MAC address of this Agent.
Last Seen	The last date and time this alarm was generated for this Agent, in the format: mm/dd/yyyy hh:mm:ss am/pm .
Critical	The number of Critical alarms generated for this Agent.
Major	The number of Major alarms generated for this Agent.
Minor	The number of Minor alarms generated for this Agent.
Ignore	The number of Ignored alarms generated for this Agent.

Using the Alarms Tab

The **Alarms** tab displays an overview of alarm activity by severity level. You can view a graph that summarizes the information or a more detailed table.

The graph shows:

- The number of alarms being generated for each severity
- The number of Agents in your AirDefense Personal system that are generating the alarms.



Right-click on one of the bars in the graph to view this information as a table.



Double-left-click on a row to view the **Agent Details** screen for that Agent.

The **Previous** and **Next** buttons page allow you to see more devices in this view. You can choose the number of device per page by selecting this from the drop-down box.

Right-click on the table to return to the graph view.



To Access the Alarms Table

To access the table, place your mouse on any bar in the graph and right-click. The table displays the following information.

Entries in the table are color-coded according to their severity level (Severe, High, Elevated, Guarded, Low).

Column	Meaning
User Name	The user name assigned to this Agent.
Computer Name	The alpha or numeric computer name of this Agent.
Threat Level	The threat level for this Agent. (Severe, High, Elevated, Guarded, or Low)
Agent ID	The MAC address of this Agent.
Last Seen	The last date and time this alarm was generated for this Agent, in the format: mm/dd/yyyy hh:mm:ss am/pm .
Critical	The number of Critical alarms generated for this Agent.
Major	The number of Major alarms generated for this Agent.
Minor	The number of Minor alarms generated for this Agent.
Ignore	The number of Ignored alarms generated for this Agent.

Chapter 5. Wizards

AirDefense Personal Manager has a series of Wizards built into the product which help the administrator easily set up the system and create new profiles for deployment.

Note: For very detailed examples see the [Policy Design Guide](#) on <http://support.airdefense.net/>.

The Wizards included with this release are:

- Rule Wizard
- Response Wizard
- Policy Wizard
- Profile Wizard
- Group Wizard

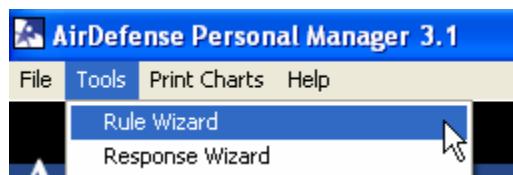
You should perform the actions in the following order:

1. Determine what corporate policy, security, and mobile enforcement.
2. Design rules around your determination.
3. Define your set of responses for various rules .
4. Create policies.
5. Create a new profile and assign the relevant policies and settings to the profile. This will be your new profile to assign new users when they first access the system.
6. Assign this profile to the Default Group.
7. Create more profiles if needed.
8. Create groups and assign the relevant profiles.
9. Move users into the relevant groups.

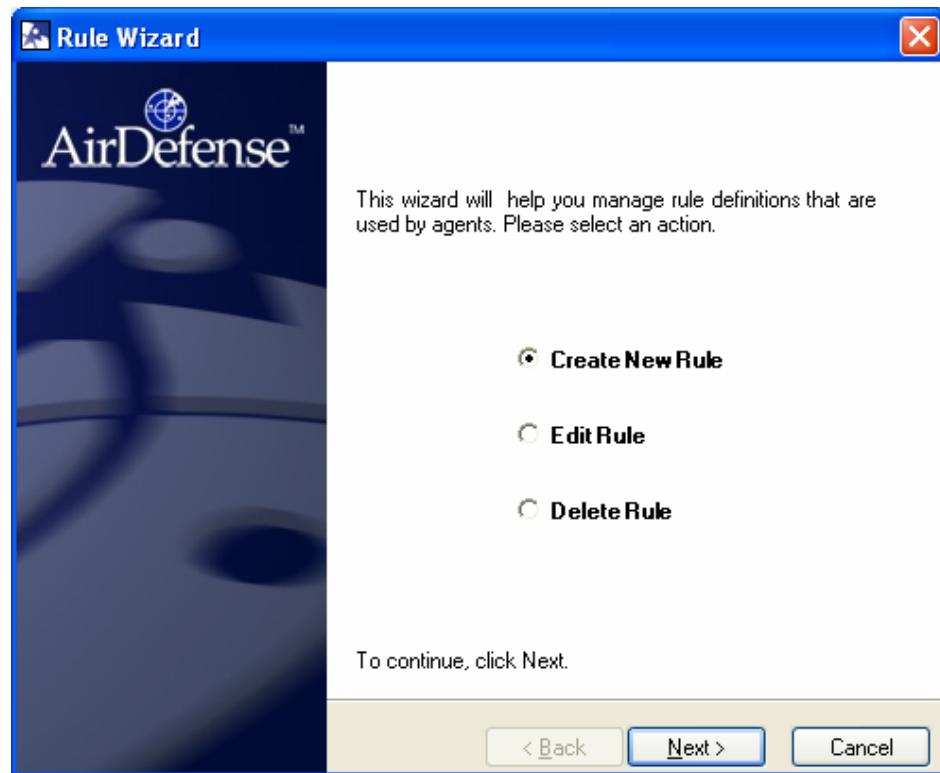
Using the Rule Wizard

To use the Rule Wizard to create, edit, or delete a custom rule, do the following:

From the **Tools** menu, pull down and select **Rule Wizard**.



When you select the Rule Wizard, the first wizard screen appears. You can click on the X in the upper right to close the screen at any time. Use the <Back> button to go back to the previous screen (not active when grayed-out).



The first wizard screen gives you three choices. To choose, click on the radio button next to the choice.

- **Create New Rule:** Choose this to create a rule.
- **Edit Rule:** Choose this to edit an already created rule.
- **Delete Rule:** Choose this to delete an already created rule.

Click **<Next>**.

New Rule or Edit Rule

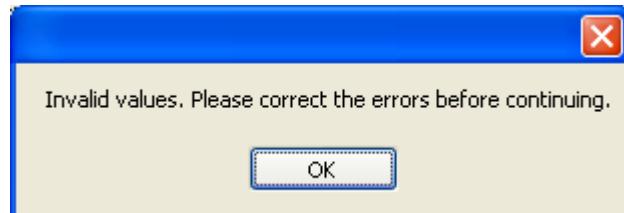
If you choose New Rule or Edit Rule, the following screen appears.

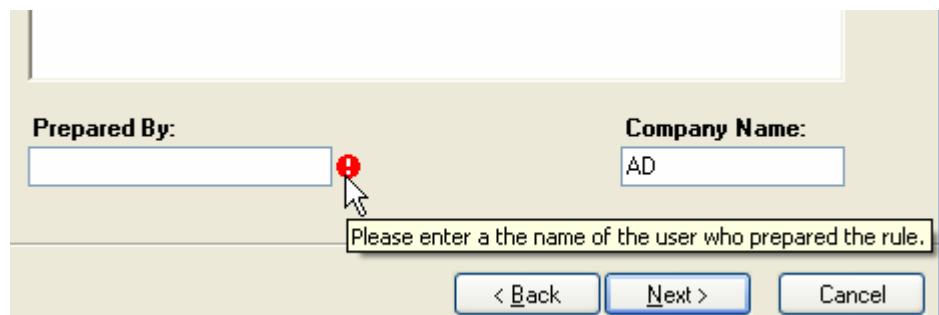


Enter new rule details in the fields (see the descriptions, below). (Some fields are required to activate the <Next> button. Use the <Back> button to go back to the previous screen.)

- **Rule Title** – This must be a unique name for the rule you are creating
- **Rule Type** – You have the following choices:
 - Hotfix
 - Process
 - Registry
 - Device
 - Network
- **Rule Description** – This is a text field where you should explain what the rule does.
- **Prepared By** – Enter the administrator's name that created the rule.
- **Company Name** – Enter the Company Name.

All of these fields are mandatory apart from the Rule Description Field. If you miss one by mistake the program will not proceed and show you where you have missed the field.

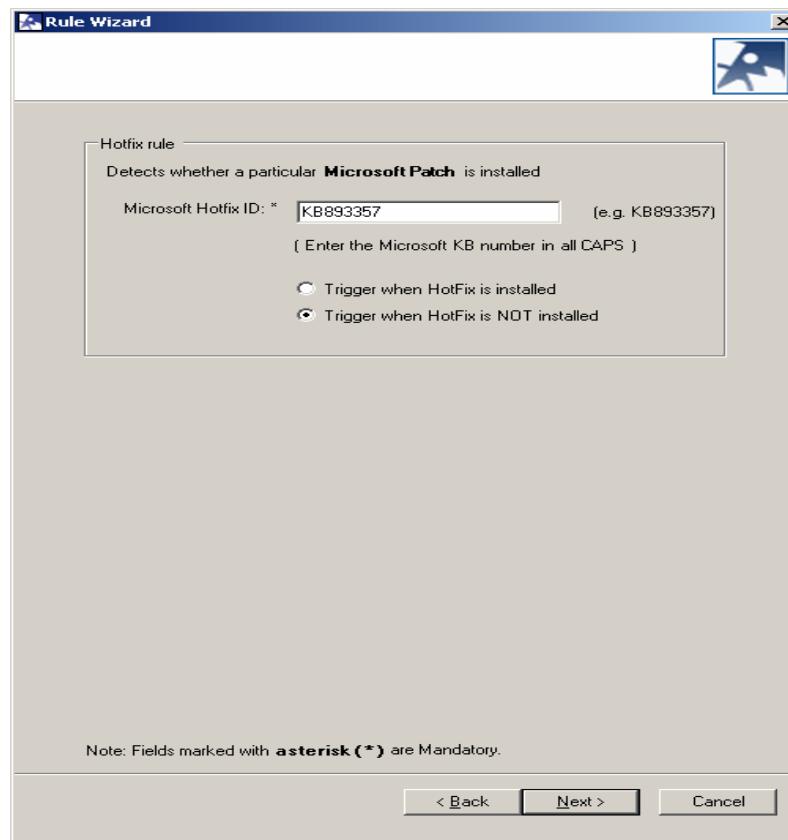




Click <Next> to proceed to the next rule information screen.

Hotfix Rule

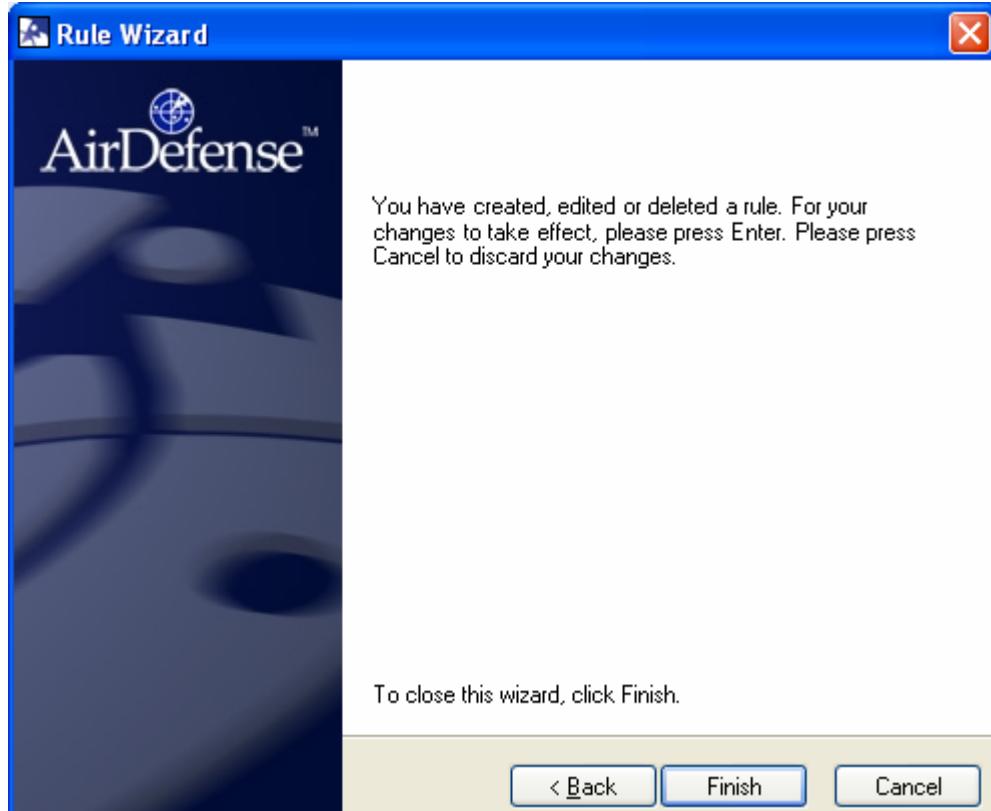
If you choose **Hotfix**, the Create Hotfix Rule screen displays.



1. In the Hotfix ID field you need to enter in the number of the Hotfix ID field (e.g. KB893357).
2. You also need to choose the trigger condition.
 - By Selecting “Trigger when Hotfix is installed”, you will return a positive detection to the agent if the Hotfix is installed.
 - By Selecting “Trigger when Hotfix is NOT installed”, you will return a positive detection to the agent if the Hotfix is NOT installed.

3. Click <Next> to proceed to the next rule information screen.

After defining all your rules, the following window display:

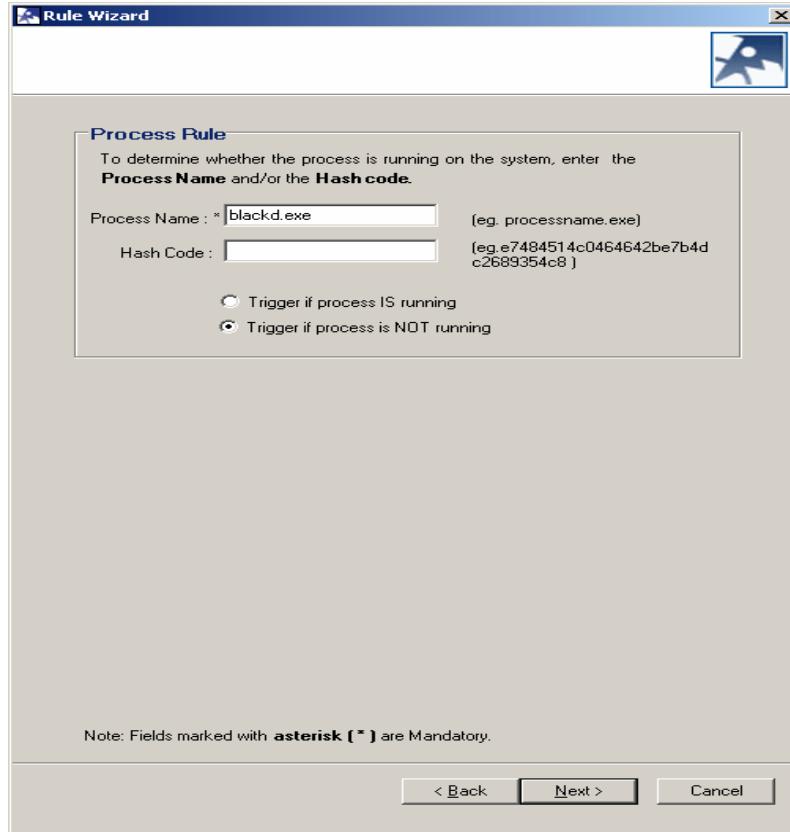


4. By Clicking <Finish> you will commit the new rule (or change if you are editing it) to the database. If you are editing a rule which already appears in at least one distributed Profile, then this will automatically update the profile as well. Then the next time the agent checks profile, it will be downloaded automatically.

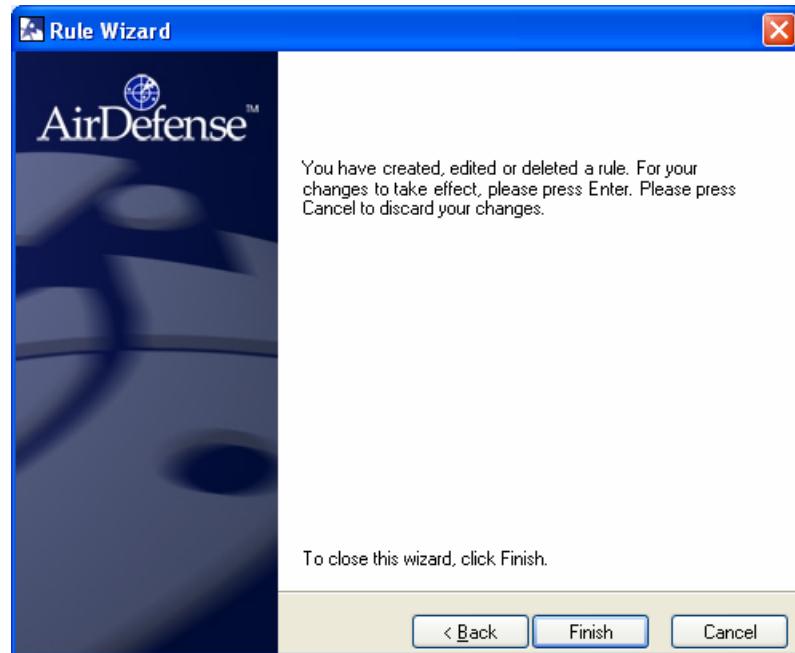
Process Rule

If you chose **Process**, the Create New Process Rule screen displays.

Click <Next> to proceed to the next rule information screen.



1. In the Process Name field enter in the name of the process to be searched for, e.g. openvpn.exe.
2. The Hash Code is optional. In this field, you can enter the MD5 checksum hash for the process. When the agent detects the process, it will run a checksum against it to make sure it really is the expected process, instead of another application masquerading as something else.
3. You also need to choose the trigger condition.
 - By Selecting “Trigger if process IS installed”, you will return a positive detection to the agent if the process is installed.
 - By Selecting “Trigger when process is NOT running”, you will return a positive detection to the agent if the process is NOT installed.

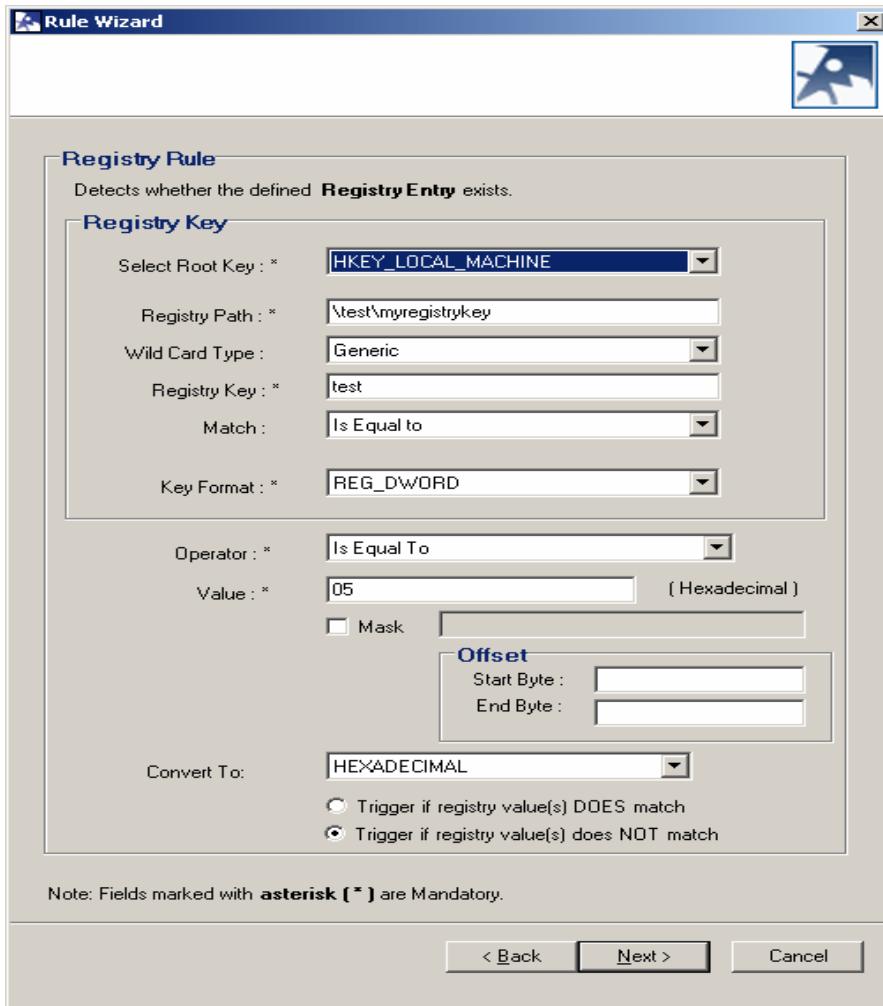


4. By Clicking <**Finish**> you will commit the new rule (or change if editing) to the database. If you are editing a rule which already appears in at least one distributed Profile, then this will automatically update the profile as well. The next time the agent reports to the server it will automatically download any updates.

Registry Rule

If you chose **Registry**, the Create New Registry Rule screen displays.

1. Click <Next> to proceed to the next rule information screen.

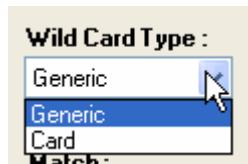


2. Enter the required registry key and then the value to compare via operator.
3. **Select Root Key:** Enter a choice for the registry key. To do this, select one of root keys from the drop-down menu.
 - HKEY_LOCAL_MACHINE
 - HKEY_CLASSES_ROOT
 - HKEY_CURRENT_USER
 - HKEY_USERS
 - HKEY_CLASSES_ROOT
 - HKEY_CURRENT_CONFIG

4. **Registry Path:** Enter a registry path.

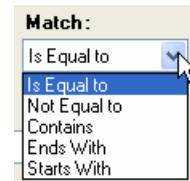
(For example, for HKEY_LOCAL_MACHINE\SOFTWARE\AirDefense Mobile\License, you would select HKEY_LOCAL_MACHINE from the drop down menu and then type SOFTWARE\AirDefense Mobile\ in the text box.)

5. **Wild Card Type:** Choose whether to use a “card” wild card type to search all keys beneath a certain registry path. The Default is “generic” which means not used.



6. **Match:** Allows more advanced filtering on the exact registry key. To do this, select an operator from the drop-down menu.

- Is Equal to
- Not Equal to
- Contains
- Ends With
- Starts With



7. **Registry Key:** Enter a text string (up to 255 characters) where the rest of the registry key can be found.

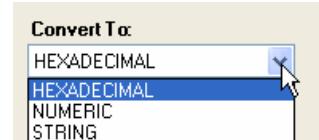
(For example, for HKEY_LOCAL_MACHINE\SOFTWARE\AirDefense Mobile\License, you would select HKEY_LOCAL_MACHINE from the drop down menu and then type **Software\AirDefenseMobile\License** in the text box.)

8. **Key Format:** Select the key format. To do this, select one of the formats from the drop-down menu.

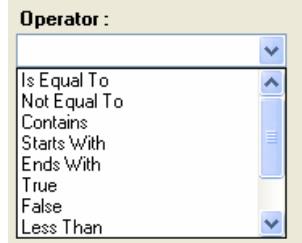
- REG_BINARY
- REG_SZ
- REG_DWORD

9. **Convert To:** Enter the format you want to change the registry key value to before checking for the value. Choices are:

- Hexadecimal
- Numeric
- String



10. **Operator:** Includes the following:



11. **Mask:** Enter the mask you require. Please note that the zero value means ignore this bit.



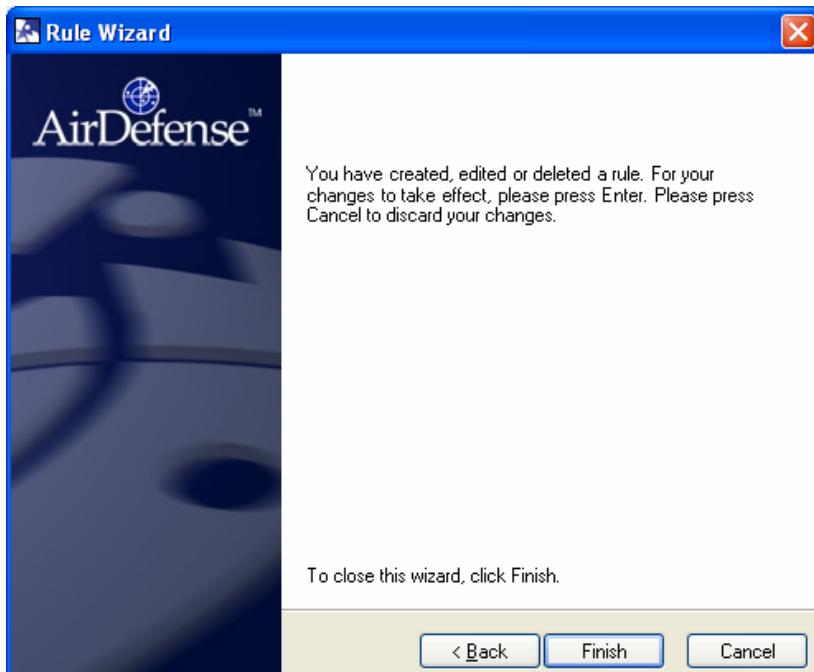
12. **Start and End:** Enter the start offset you wish to start matching, with an optional End offset if needed.

13. **Value:** Enter the registry value to search for. The value will depend on your choice for Key Format. (For example, if REG_DWORD was chosen, then a text input box is needed along with a radio button for decimal or hexadecimal translation.)

14. You also need to choose the trigger condition.

- By Selecting “Trigger if registry value(s) DOES match”, you will return a positive detection to the agent if the process is installed.
- By Selecting “Trigger if registry value(s) does NOT match”, you will return a positive detection to the agent if the process is NOT installed.

15. Click <Next>.

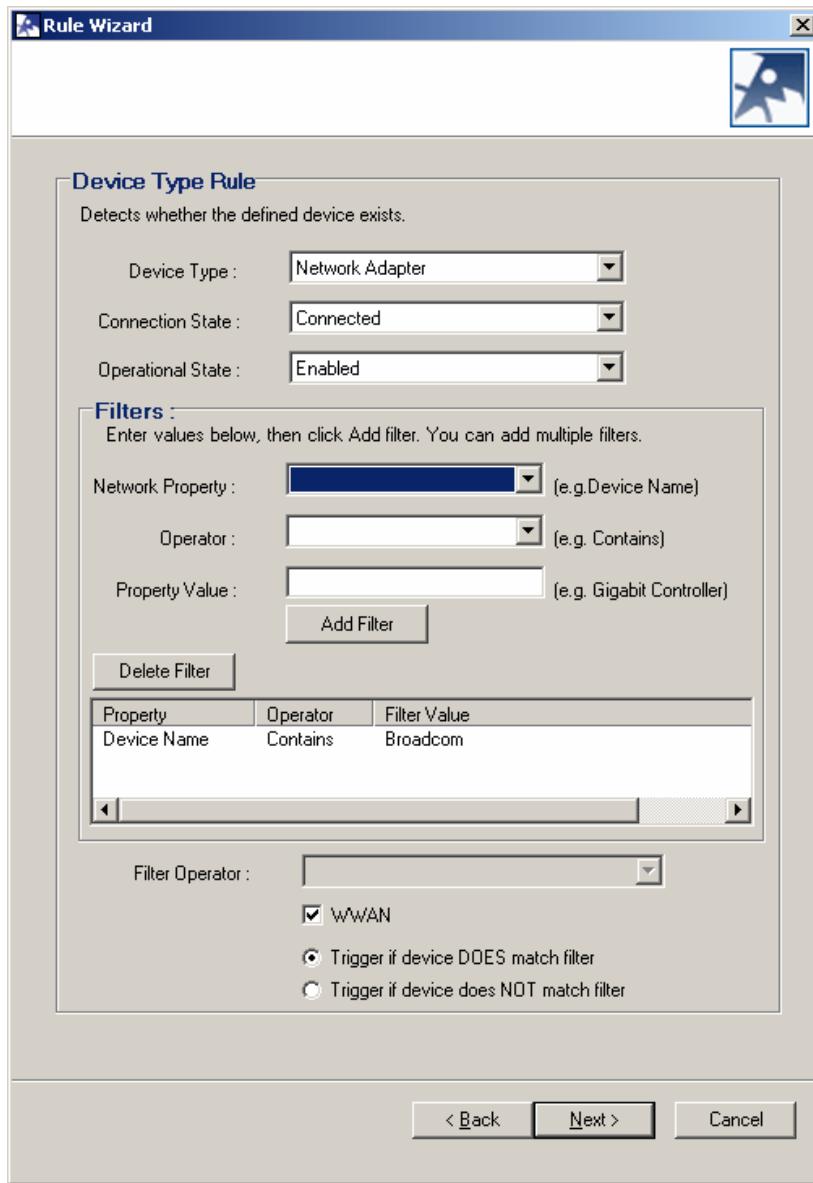


16. By Clicking <Finish> you will commit the new rule (or change if editing) to the database. If you are editing a rule which already appears in at least one distributed Profile, then this will automatically update the profile as well. The next time the agent reports to the server it will automatically download any updates.

Device Rule

If you choose **Device**, the Create New Registry Rule screen displays.

Click <Next> to proceed to the next rule information screen.



The Device Rule is used to look at the various types of network adapters in your system and then provide information about their connection and operational states. This rule is useful in detecting non-Ethernet adapters such as Wireless WAN adapters (e.g. EV-DO or 3G adapters) because Windows does not provide a mechanism to differentiate these from normal modems. By looking for certain text strings within the name of the adapter it is very easy to build up a rule which can identify the Wireless WAN cards available in your country.

- **Device Type:** Can be Any, Modem or Network Adapter
- **Connection State:** Can be Any, Disconnected or Connected
- **Operational State:** Can be Any, Enabled or Disabled

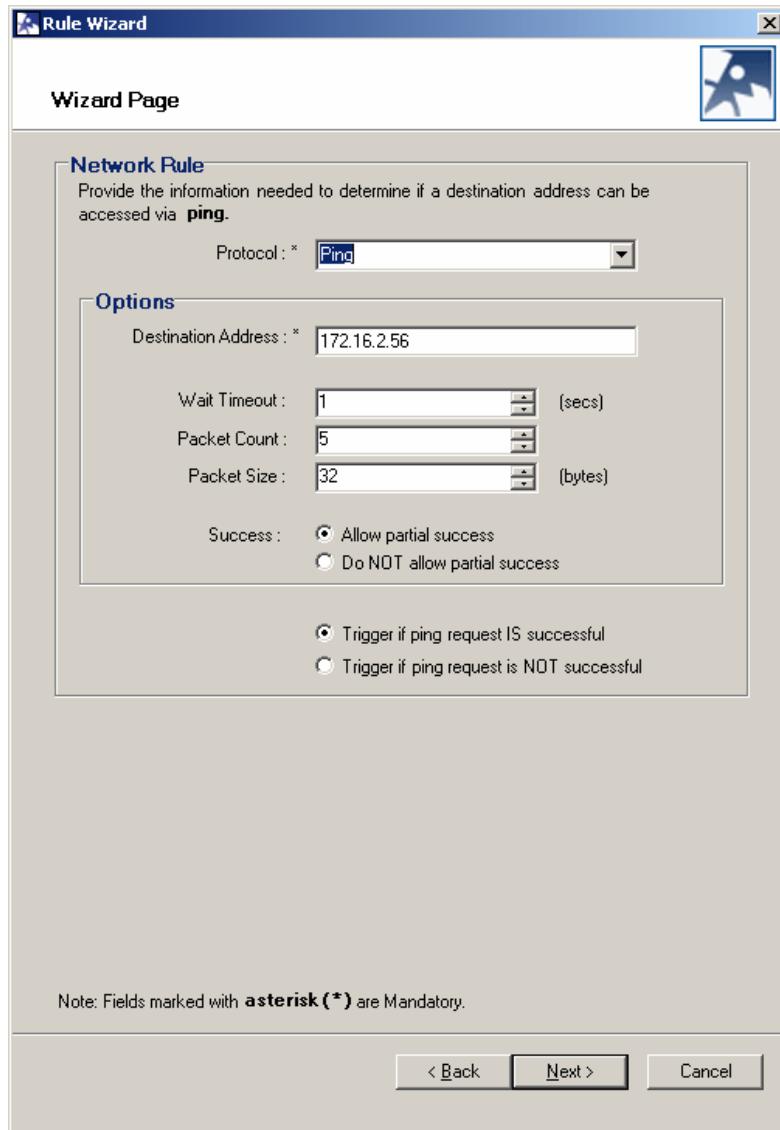
Filters can then be applied based on the name of adapter.

- **Network Property:** Can be Device Name
- **Operator:** Can be Is Equal to, Not Equal to, Contains, Starts with and Ends with
- **Filter Value:** User defined
 - Multiple values can be added using the **Add Filter** button and a Boolean operation can be chosen based on **AND** or **OR**. Filters can also be removed by clicking on the **Remove Filter** button.
 - An optional checkbox is there if this new rule is looking for Wireless WAN (WWAN) adapters. This is needed if you want to enforce the simultaneous wired and WWAN or simultaneous wireless and WWAN policies.
 - You also need to choose the trigger condition.
- By Selecting “Trigger if device DOES match filter”, you will return a positive detection to the agent if the device name filter, Device Type, Connection State and Operational State matches the values and operator.
- By Selecting “Trigger if device does NOT match filter”, you will return a positive detection to the agent if the device name filter, Device Type, Connection State and Operational State does not match the values and operator.

Network Rule

If you chose **Network**, the Create New Network Rule screen displays.

Click <Next> to proceed to the next rule information screen.



The Network rule is used to create ping tests to defined addresses. This test can be used to reach specific networks that may only be available when you have access to a corporate network (either directly or via a VPN).

Note: Currently, the only protocol available in the Network Rule Wizard is ping.

Fill in the following parameters:

- **Destination Address:** This address can either be an IP address in the xxx.xxx.xxx.xxx format or a name such as www.airdefense.net.

- **Wait Timeout:** This is how long the agent should wait before determining the ping has failed to reach its destination. The value is in seconds (1 sec default).
- **Packet Count:** This is how many times we should do the test. (5 is the default).
- **Packet Size:** This is the size in bytes of the ping packet (32 bytes is the default).
- **Allow Partial Success:** These radio buttons allow you to specify (by clicking Yes) if you will allow at least one successful ping out of the test to pass, or if all pings must pass to be successful.

You also need to choose the trigger condition.

- By Selecting “Trigger if ping request IS successful”, you will return a positive detection to the agent if the device name filter, Device Type, Connection State and Operational State matches the values and operator.
- By Selecting “Trigger if ping request is NOT successful”, you will return a positive detection to the agent if the device name filter, Device Type, Connection State and Operational State does not match the values and operator.

Delete Rule

If you choose **Delete Rule**, the following screen appears.

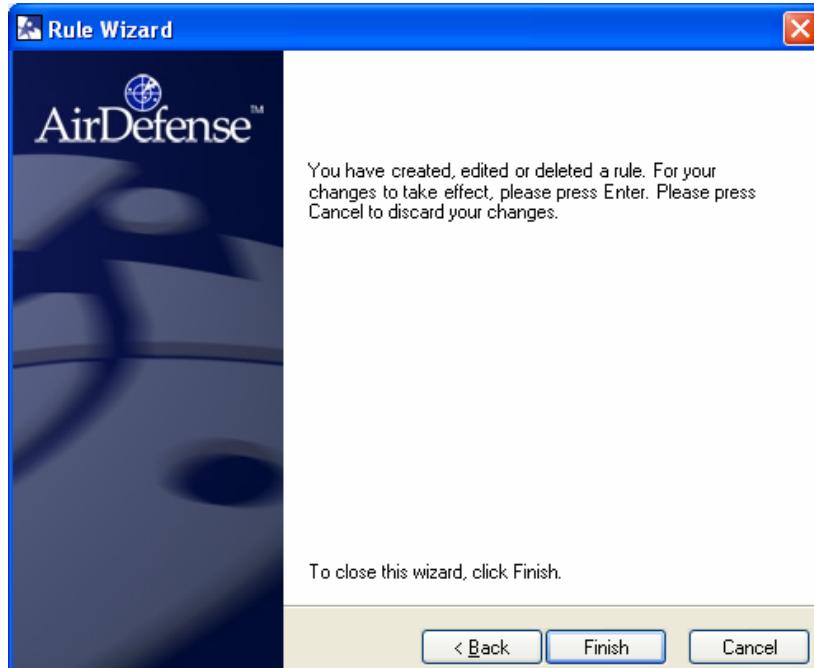


From the Rule Title drop down list, select the rule you want to delete from the database and then click <**Next**>.

If you are deleting a rule which already appears in at least one distributed Profile, then you will be presented with a warning that informs you that this rule is being used and it must be removed from a policy before it can be deleted.



Otherwise the finish screen will be presented.



Click the <Finish> button to delete this rule from the database.

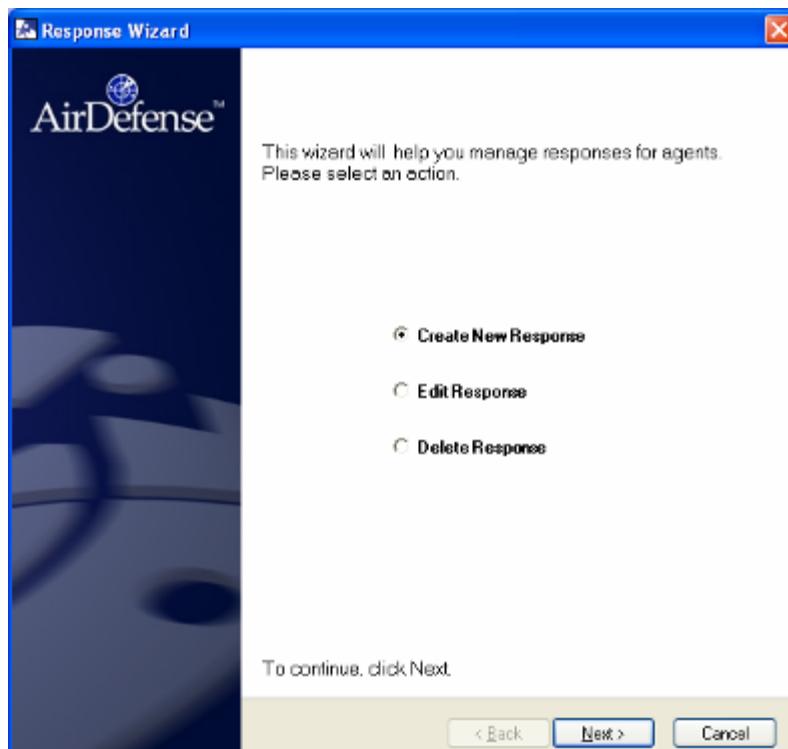
Response Wizard

Using the Response Wizard

To use the Custom Rule Wizard to create, edit, or delete a custom rule, do the following:

1. From the **Tools** menu, pull down and select **Rule Wizard**.

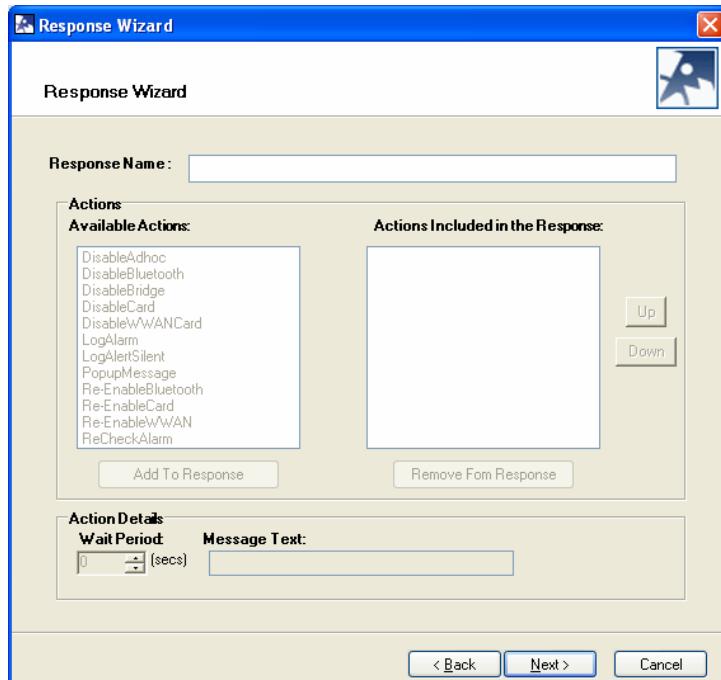
When you select the Response Wizard, the first wizard screen appears. You can click on the **X** in the upper right to close the screen at any time. Use the **<Back>** button to go back to the previous screen (not active when grayed-out).



2. The first wizard screen gives you the following choices. Make a selection from the radio button options:
 - **Create New Response:** Choose this to create a rule.
 - **Edit Response:** Choose this to edit an already created rule.
 - **Delete Response:** Choose this to delete an already created rule.
 - Click **<Next>**.

New Response or Edit Response

If you choose New Response or Edit Response, the following screen appears.



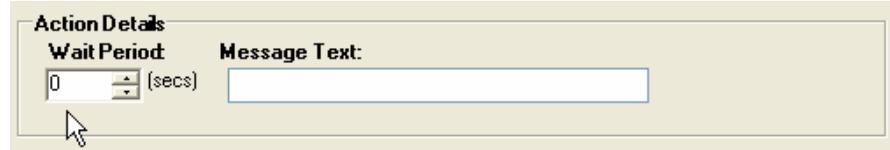
1. Type in a unique name in the Response Name field.
2. Select the response you want to from the choices available.
 - **DisableAdhoc** – This can be used to disable the setting in the Windows Zero Configuration Client which allows Ad-Hoc connections to be formed. This is only supported currently in this supplicant and will not work for other supplicants.
 - **DisableBluetooth** – This will disable the Bluetooth adapter.
 - **Disable Bridge** – This will disable bridges set up between two different adapters on the same system.
 - **Disable Card** – Disables the currently active Wireless LAN adapter
 - **DisableWWANCard** – Disables the currently active WWAN adapter
 - **Log Alarm** – Logs the alarm in the system
 - **Log Alert Silently** – Logs the alarm, but nothing is seen on the agent
 - **PopupMessage** – Pops up a message in the lower-right hand corner of the user's screen. The message will appear on top of any other windows and will remain there until the user clicks on it.
 - **Re-EnableBluetooth** – Re-enables the Bluetooth adapter.
 - **Re-Enable Card** – Re-Enables the current disabled Wireless LAN adapter
 - **Re-EnableWWAN** – Re-enables the wireless WAN adapter.

- **ReCheck Alarm** – ReChecks the same Policy to see if it is still being raised (usually used with the wait state to recheck the policy after X secs).

3. Add more actions until you are done.

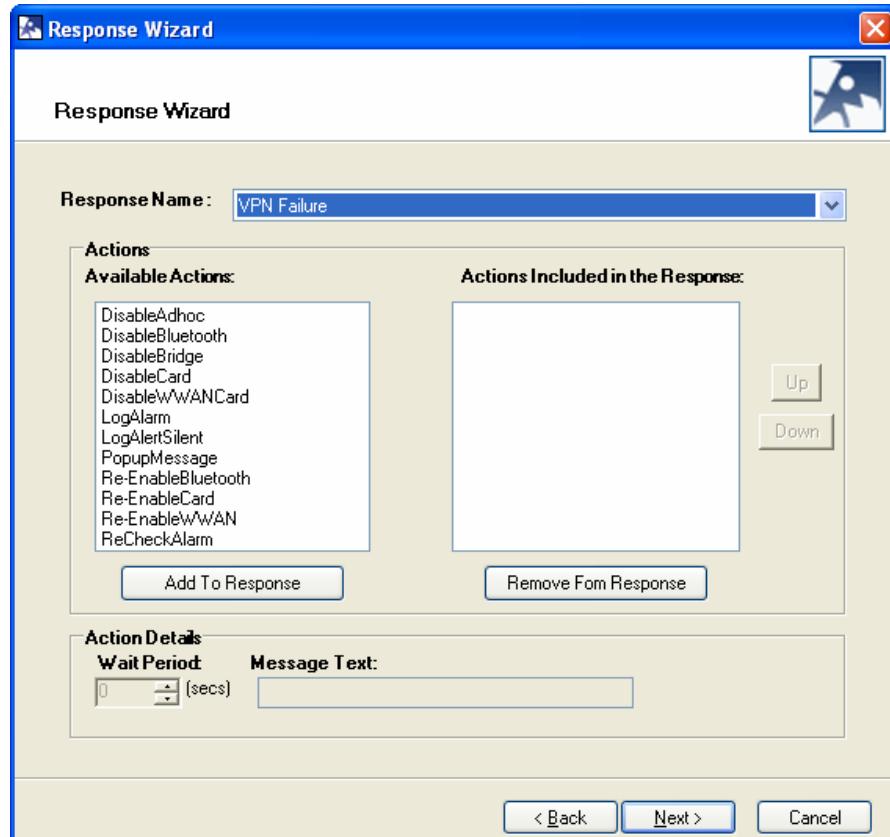
Action Details

Please note that you can only use the message text with popup message action. Also the Wait Period is always applied BEFORE taking the action.



Delete Response

If you choose **Delete Response**, the following screen appears.



1. Choose the Response you want to delete from the drop down list then click <**Next**>.
2. Click <**Finish**> to delete the response.

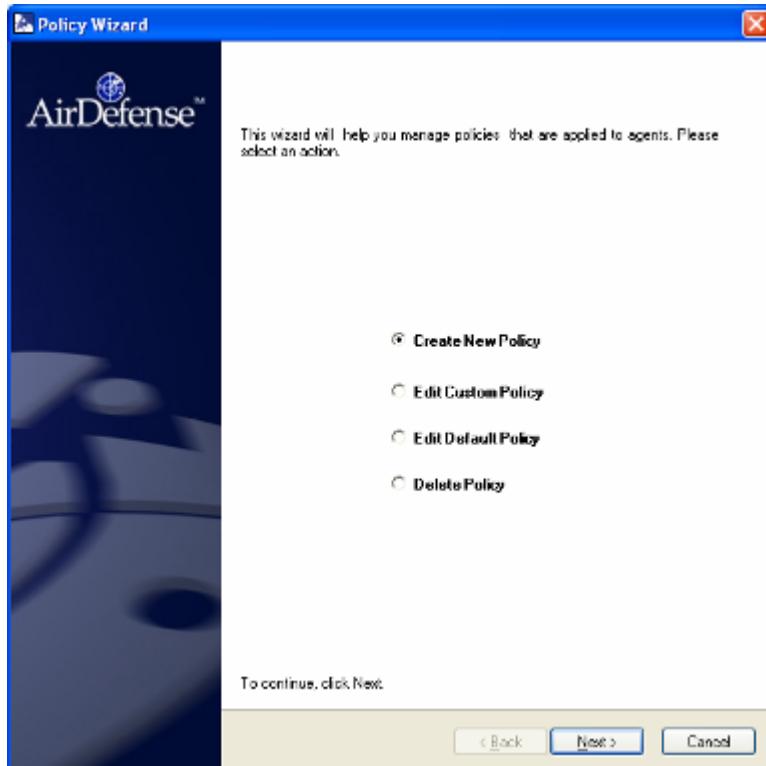
Policy Wizard

Using Policy Wizard

To use the Policy Wizard to create, edit, or delete a policy, do the following:

From the Tools menu, pull down and select **Policy Wizard**.

When you select the Policy Wizard, the first wizard screen appears. You can click on the **X** in the upper right to close the screen at any time. Use the <Back> button to go back to the previous screen (not active when grayed-out).



The first wizard screen presents the following choices. To choose, click on the radio button next to the correct selection.

- Create New Policy: create a new policy
- Edit Custom Policy: edit an already created policy
- Edit Default Policy: edit the response to a Default policy
- Delete Policy: delete an already created policy

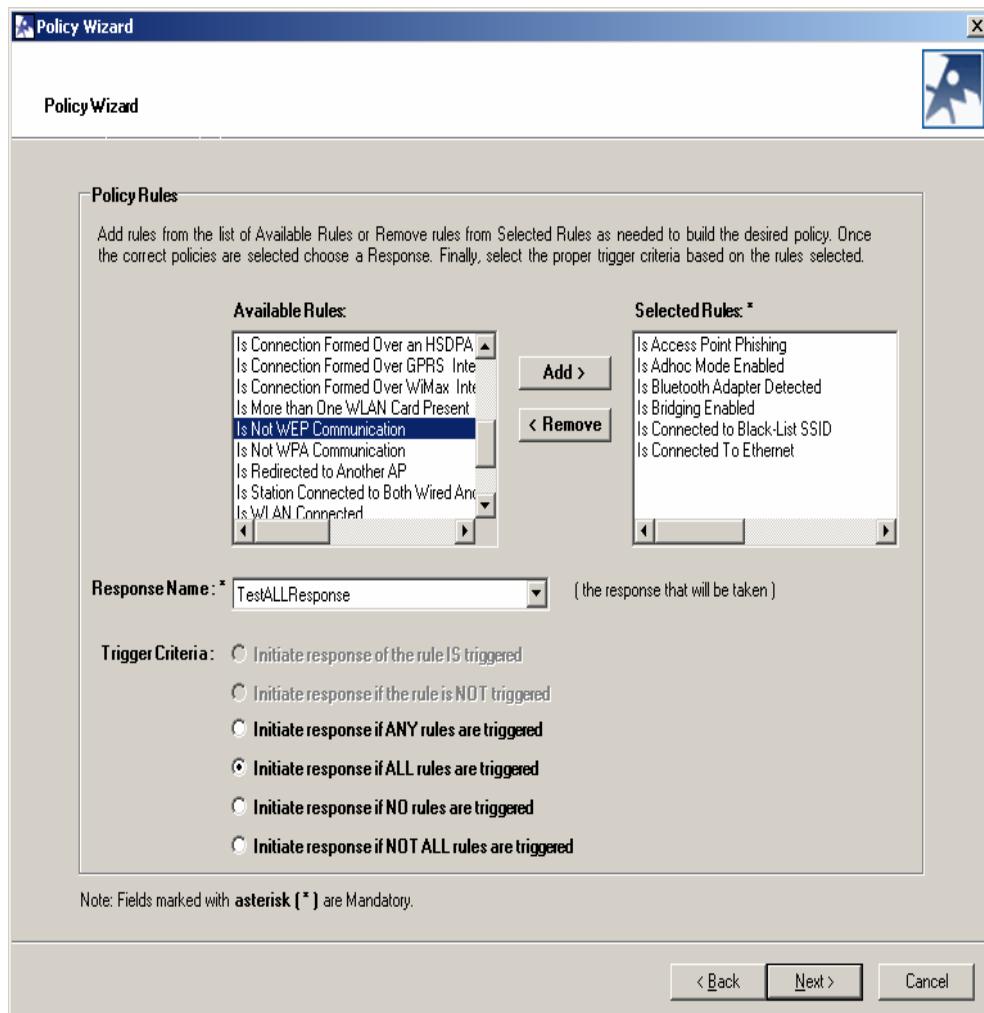
New Policy or Edit Custom Policy

1. Choose New Policy or Edit Policy, the following screen appears.

The screenshot shows the 'Policy Wizard' window. At the top, it says 'Prepared By: * [Chris]' and 'Company Name: * [YourCompanyNameHere]'. Below that is a section titled 'Policy Details' containing 'Policy Name: * [MyTestPolicy]', 'Policy Description: [Enter a description of the policy]', 'Issue: [Describe what possible issues can be affected]', 'Solution: [describe a possible solution and the steps involved]', and 'Category: * [Suspicious WLAN Settings]'. A note at the bottom left says 'Note: Fields marked with asterisk [*] are Mandatory.' At the bottom right are buttons for '< Back', 'Next >', and 'Cancel'.

- **Prepared By** – Enter the administrator's name that created the rule.
- **Company Name** – Enter the Company Name the rule applies to here.
- **Policy Name** – Enter a name for this alarm set.
- **Policy Description** – This is a text field where you should explain what the policy does for other administrators to view.
- **Issue** – Insert descriptive text for a likely cause.
- **Solution** – Insert descriptive text for a potential remedy.
- **Category** – Select one of four categories to assign the alarm set.

2. Click <Next>.



- **Available Rules:** This list box displays all rules available for use within a policy.
- **Selected Rules:** This list box contains all the rules that are selected to use within a policy.
- **Response Name:** Choose from the drop-down box of defined responses.
- **Policy Rules to be included:** Each policy needs at least one rule. You can select **this** one rule from the list of available rules by using the arrow buttons. Transfer the rule into the alarm set as desired. If you just select one rule, the screen remains the same. If you select more than one rule, the **Trigger Criteria** field becomes active. You must select an **ANY, ALL, NO, NOT ALL** actions to determine how your policies relate to each other. (See example below)

The following example shows a set of 3 rules. Each rule is set to trigger if a process is running. The next 4 columns show when a policy will fire a determined response based on choices made during policy creation policy.

Example Rules and Policy operator						
R1 (Process 1)	R2 (Process 2)	R3 (Process 3)	ANY	ALL	NO	NotAll
TRUE	TRUE	TRUE	triggers	triggers	does not Trigger	does not trigger
FALSE	TRUE	TRUE	triggers	does not trigger	does not trigger	triggers
TRUE	FALSE	TRUE	triggers	does not trigger	does not trigger	triggers
TRUE	TRUE	FALSE	triggers	does not trigger	does not trigger	triggers
FALSE	FALSE	TRUE	triggers	does not trigger	does not trigger	triggers
TRUE	FALSE	FALSE	triggers	does not trigger	does not trigger	triggers
FALSE	TRUE	FALSE	triggers	does not trigger	does not trigger	triggers
FALSE	FALSE	FALSE	does not trigger	does not trigger	triggers	triggers
**Rules Set for to Trigger if process is running						

The above example can be used to explain a situation where a user wants to monitor 3 processes. Depending on the requirements the user may want **ANY**, **ALL**, **NO**, or **NotAll** processes to be running.

In this particular case the user has selected to check if a process is running and to return a positive detection to each rule if the process (1-3) is found to be running.

The user can then base his/her response on the operators available. For example let's say that processes (1-3) are all related to a security application. As long as all 3 are running the program is operating normally. However, if any of the 3 go down an alarm is required. Selecting the **NotAll** operator satisfies this requirement.

Another user may be satisfied if at least one of the 3 processes is running regardless of which one, but at no time should all 3 be down at once. In this case the user may choose the **NO** operator so that a response will only be fired if no processes are detected.

There are many other combinations possible and it is left to the user to work through examples that are needed in their environment.

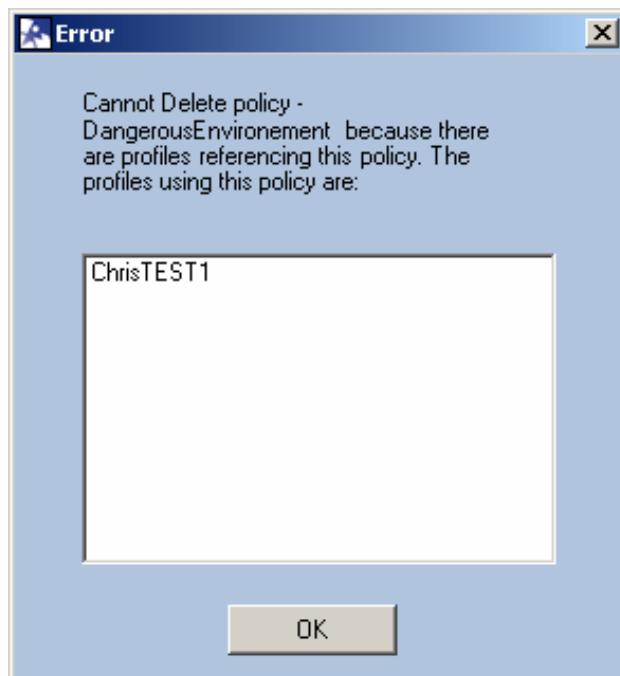
Delete Policy

If you choose **Delete Policy**, the following screen appears.

From the drop down list in the Policy Name box, select the policy you want to delete from the database and then click <**Next**>.

If you are deleting a policy which already appears in at least one Profile, then you will be presented with a warning that informs you that this policy is being used and it must be removed before it can be deleted.

Otherwise, click <**Next**>.to finish.



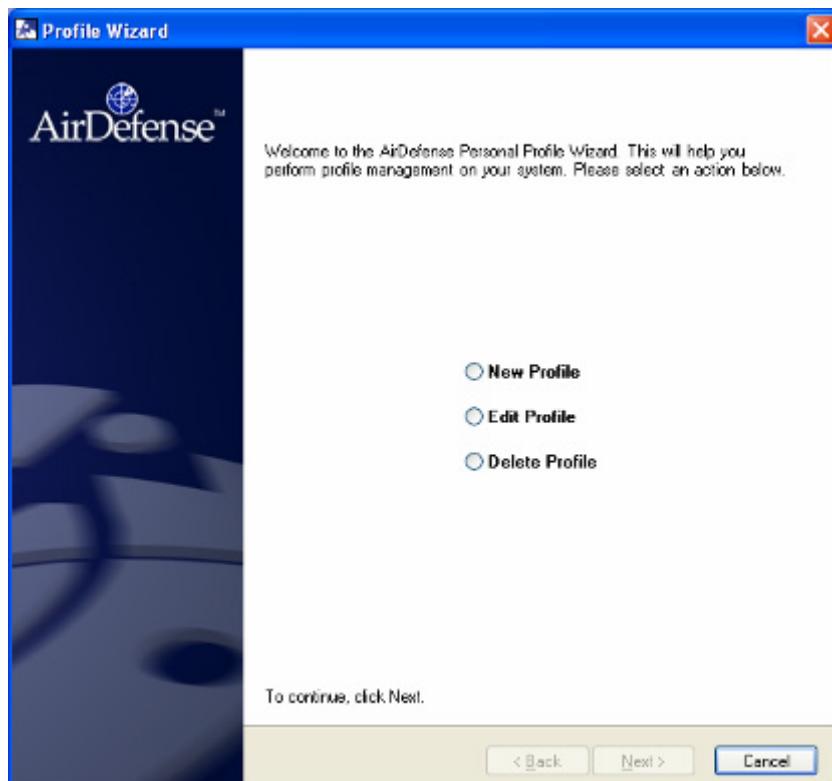
Profile Wizard

Using the Profile Wizard

To use the Profile Wizard to create, edit, or delete a policy, do the following:

From the Tools menu, pull down and select **Profile Wizard**.

When you select the Profile Wizard, the first wizard screen appears. You can click on the **X** in the upper right to close the screen at any time. Use the <**Back**> button to go back to the previous screen (not active when grayed-out).

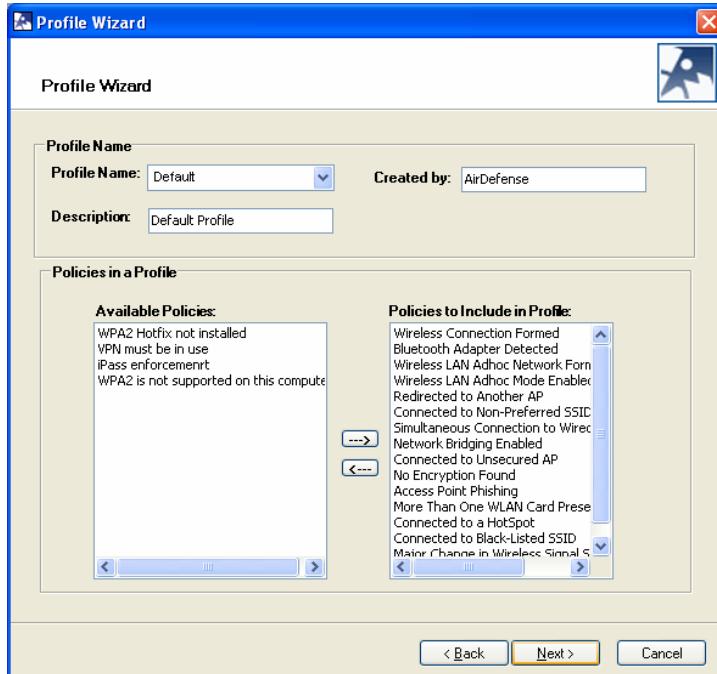


The first wizard screen gives you three choices. To choose, click on the radio button next to the choice.

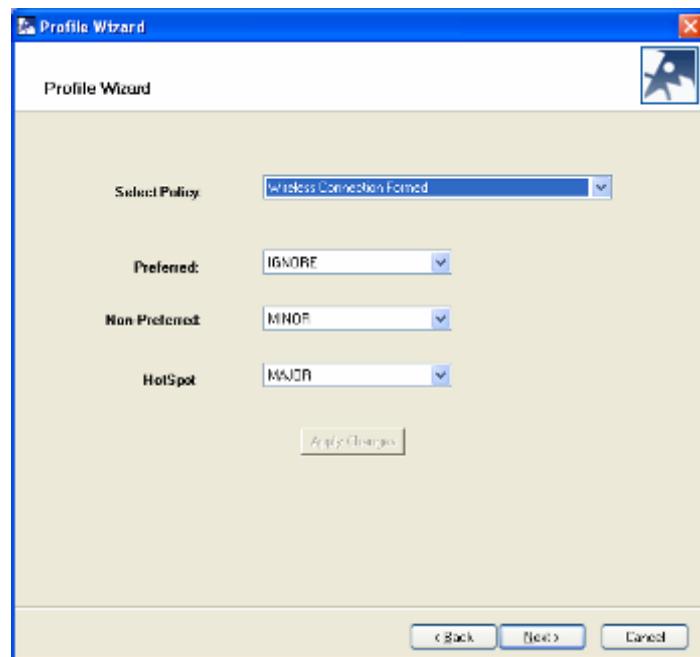
- New Profile: Choose this to create a new profile
- Edit Profile: Choose this to edit an already created policy
- Delete Profile: Choose this to delete an already created policy

Create New Profile or Edit Profile

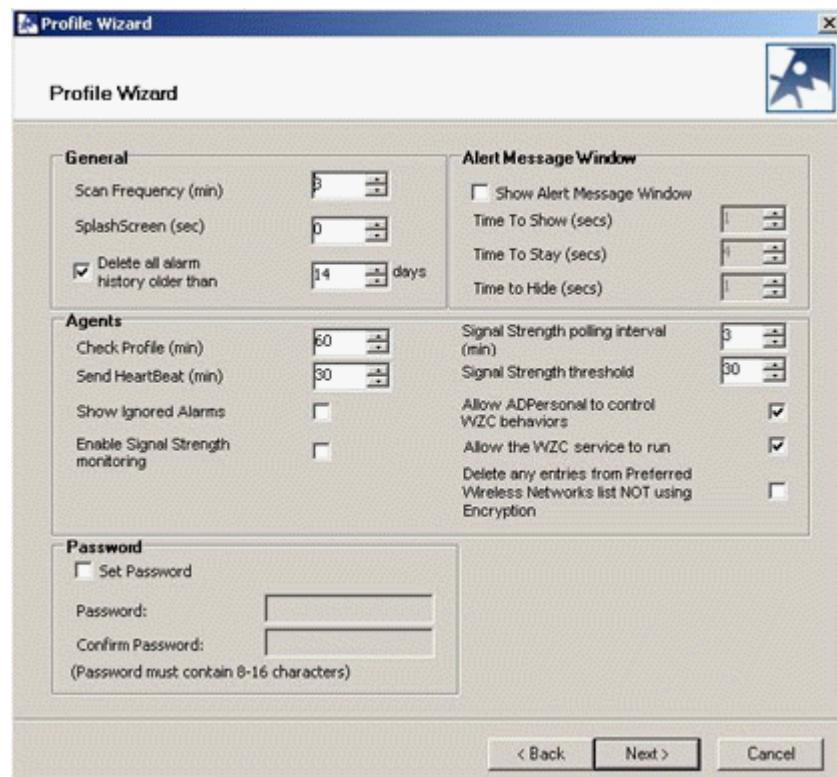
If you choose New Profile or Edit Profile, the following screen appears.



1. You need to assign a new unique name to the profile if you are creating a new Profile. Delete Default in the Profile name.
2. By default all of AirDefense's inbuilt policies will be included in the profile. You can choose to move these out of the profile if you do not wish to run them. You can then also move any of your custom policies you have created over to the right for inclusion in the profile.
3. Click <Next>.



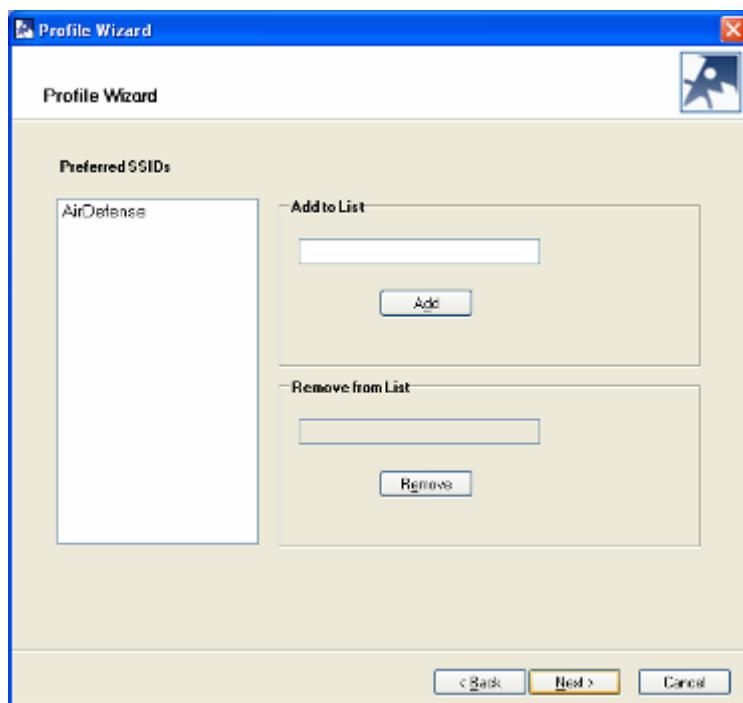
4. On the next screen you can drop down and choose any policy included in the profile and edit the alarm severities for each of the three wireless states of the agent. If you make any changes, you MUST click <Apply Changes> after each change made.
5. Click <Next> to continue.



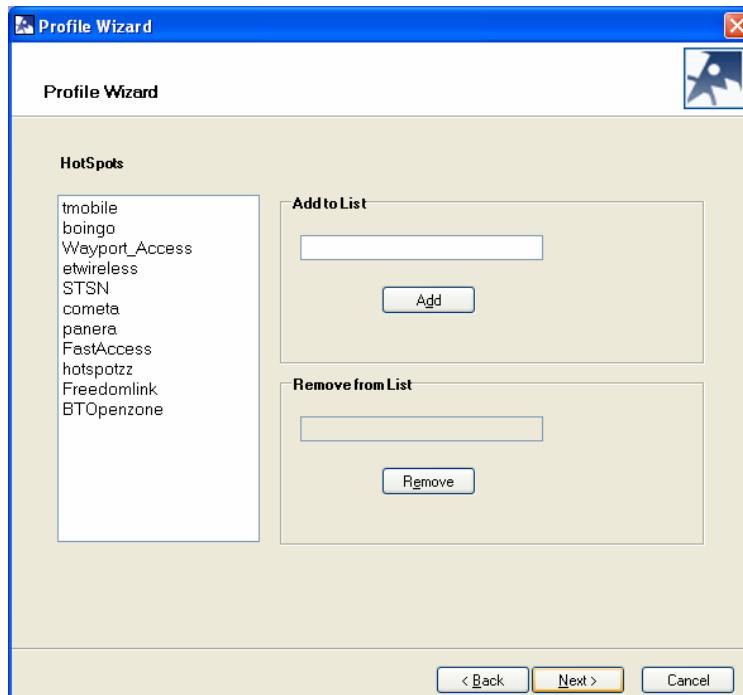
This window is divided into following four sections:

Section	Description
General	<p>Set the following options:</p> <ul style="list-style-type: none"> • Scan Frequency sets the frequency rate (in minutes) of the scans. • SplashScreen determines how long the splash screen is displayed (in seconds) when accessing the GUI. • Delete all alarm history older than specifies how many days to keep alarm history data before deleting it.
Alert Message Window	Specify if you want to display alert messages when they occur and how long to display the message. Check the checkbox to turn this feature on and then specify the times in seconds.
Agents	<p>Set the following agent settings:</p> <ul style="list-style-type: none"> • Specify time intervals for the following fields: Check Profile, Send HeartBeat, and Signal Strength polling interval. • Specify the Signal Strength threshold. • Check the checkbox for Show ignored Alarms if you want to show ignored alarms. • Check the checkbox for Enable Signal Strength monitoring if you want to monitor signal strength. • Check the checkboxes for Allow the WZC service to run and Allow ADPersonal to control WZC behaviors if you want to use WZC service. • Check the checkbox for Delete any entries from Preferred Wireless Networks list NOT using Encryption if you only want devices on your network using an encryption method.
Password	Check the checkbox to Set Password if you want the profile to have password protection and then specify a password by entering it in twice.

6. Click <Next> to continue.

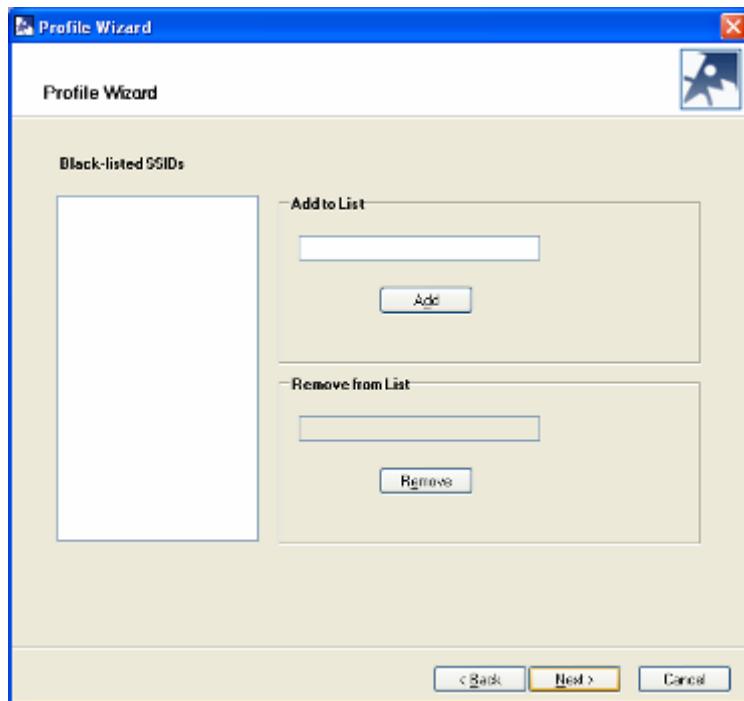


7. On this screen you can add in any Preferred SSID you want. Please note that the check is CASE-SENSITIVE.
8. Click <Next> to continue.



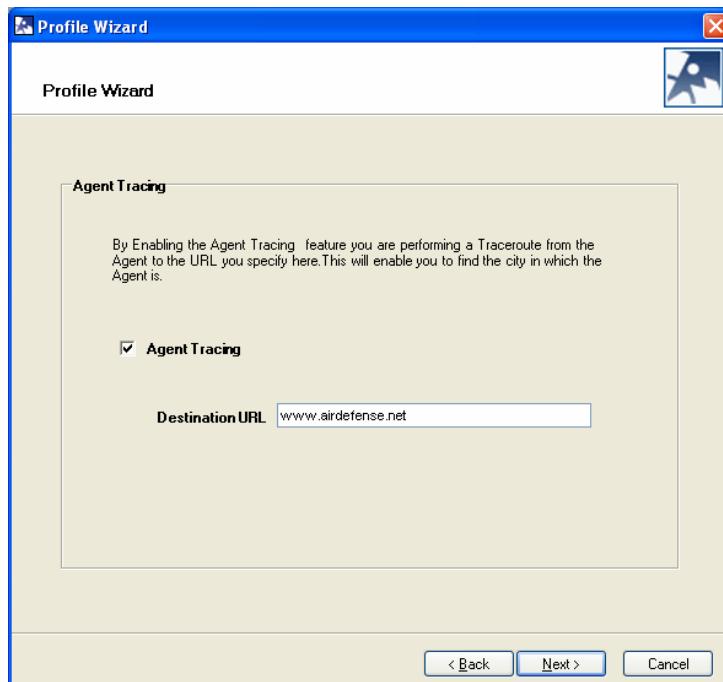
9. On this screen, you can add in any Hotspot SSID you want. Please note that the check is CASE-SENSITIVE. This can be used to differentiate between a non-preferred SSID and a genuine hotspot, although most customers treat both hotspot and non-preferred SSIDs as the same in terms of a security risk.

10. Click <Next> to continue.



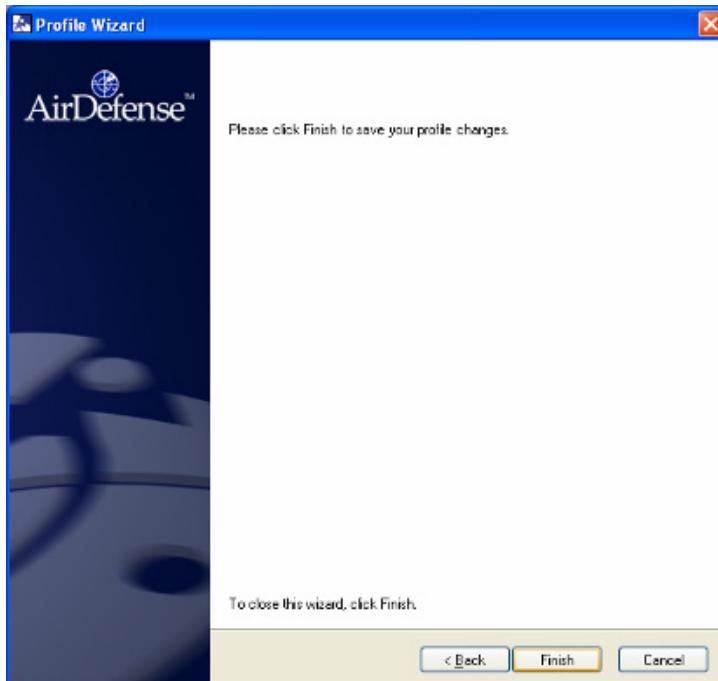
11. You can add Black-listed SSIDs here. Commonly these are networks from neighbors or internal Guest Wireless VLANs which you don't want your own users to have access to. Commonly people will use the disable Wireless Card action with the Connected to Black-listed SSID alarm.

12. Click <Next> to continue.



13. You can optionally enable the Agent tracing feature. You need to tick the check box and add in a URL or IP address which the agent can trace route back to. This information will be sent back with the alerts to the central server. The server will then try to find out which city/country the agent was in at the time.

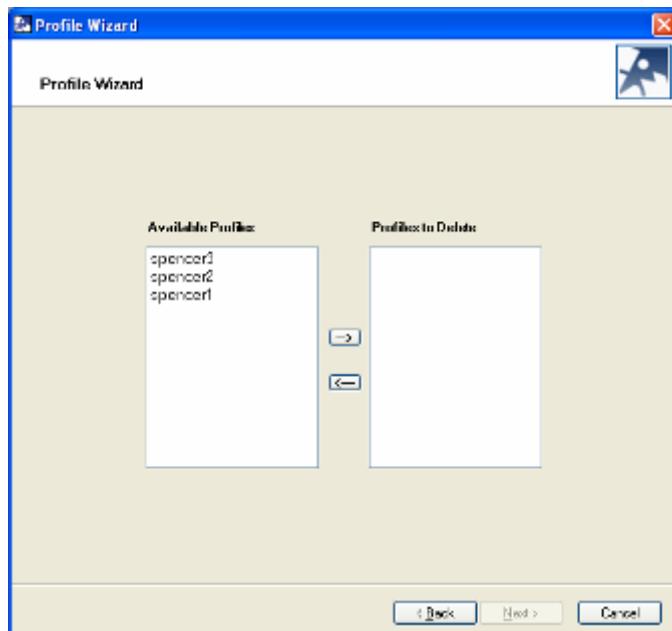
14. Click <Next> to continue.



15. Click <Finish> to create/edit the Profile.

Delete Profile

If you choose **Delete Profile**, the following screen appears.



1. Select the profile you want to delete and click the left-hand arrow to move it across to the right box. You can move multiple profiles across.
2. If a profile is assigned to a group you cannot delete it. Assign a different profile to the group before you continue.
3. Click the <**Next**> button to continue.
4. Click on <**Finish**> to delete the Profile.

Group Wizard

AirDefense Personal Manager provides a Groups Wizard that enables you to easily create, edit, or delete custom Groups.

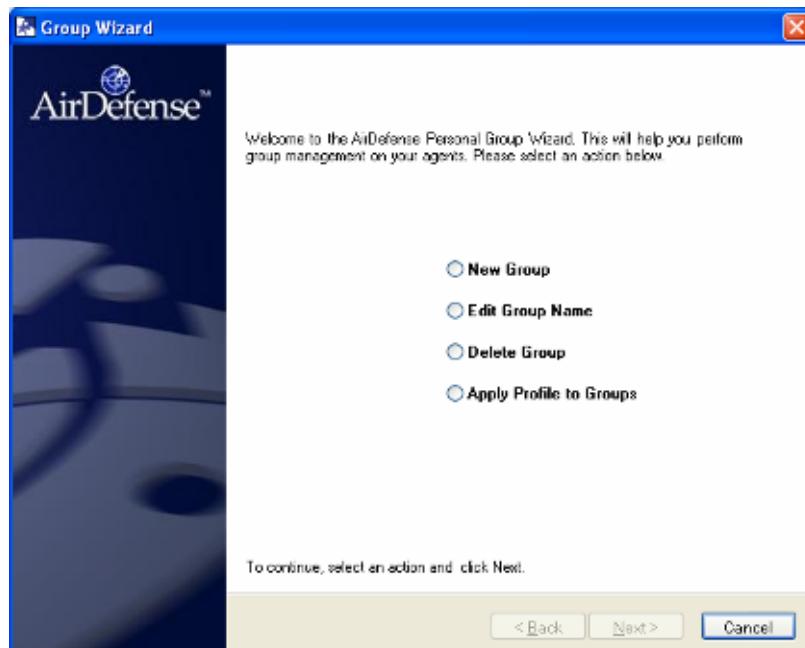
Groups Wizard

To use the Groups Wizard to create, edit, or delete a group, do the following:

1. From the Tools menu, pull down and select Group Wizard.



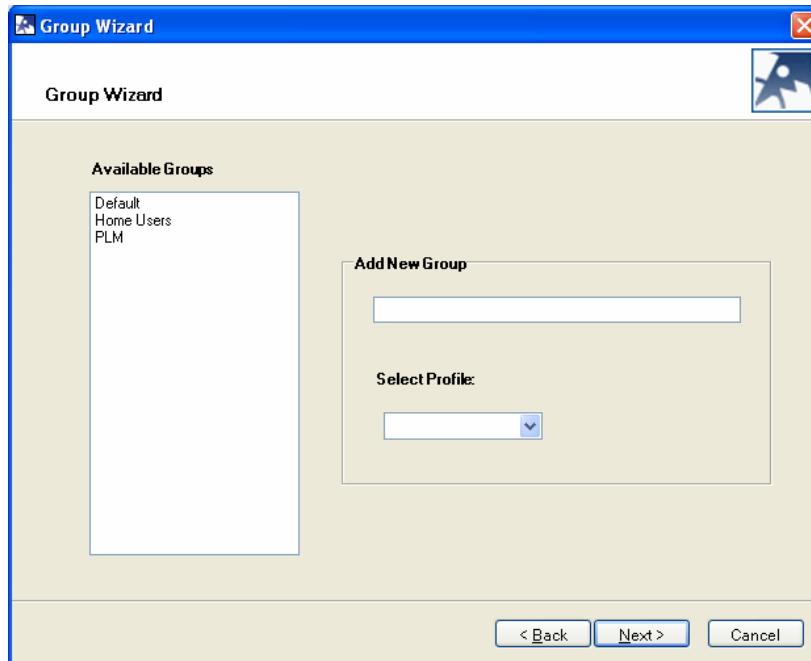
2. The first wizard screen gives you four choices. To choose, click on the radio button next to the choice.
 - **New Group:** Choose this to create a new group
 - **Edit Group:** Choose this to edit an already created Group
 - **Delete Group:** Choose this to delete an already created Group
 - **Apply Profile to Group:** Choose this to apply a profile to a Group



3. Click <Next> to continue.

New Group

If you choose a New Group, the following screen appears:



1. Add the new group name.
2. From the drop down list select the profile you want to assign to this group.
3. Click <Next>.
4. Click <Finish>.

The new group will appear in the tree. You can transfer agents into the group by selecting the agent dragging it into the group.

If you delete a group, its agents will go under the default group.

AirDefense Personal 3.4 User Manual
Issue 1.0
May 2007



4800 North Point Parkway, Alpharetta, Georgia *SA 30022 880.663.8115
www.airdefense.net info@airdefense.net